Identity Management for true system interoperability at Blackpool & The Fylde College

- a JISC "Pathfinder" & "Pilot" Project on five years development.

Author – Simon Bailey – Network Manager at Blackpool & The Fylde College

Why did we go for an FSD approach?

The strategy based on Identity Management emerged at Blackpool & The Fylde College for several reasons. By 2004 senior managers were becoming increasingly frustrated by the lack of common interface between key business systems leading to duplication of effort, inconsistent and potentially inaccurate data and a lack of a central source of management information. After significant investment in new systems and infrastructure there remained however the inability to transfer data between systems was increasing rather than decreasing had been made A clear vision by the IT department saw the inherent value in obtaining definitive data about users and presenting services to those users based on actual business process. A recurrent theme at institutions where there are a large number of users that require varying levels of access to a wide range of IT service provision is that data about any given user is often copied between systems on an as-needs basis, rather than try to fit an organisational strategy where information is collected once from a definitive/authoritative source. The other main aspect, which was becoming evident in some areas of corporate business support, was that defined business process was sometimes a little vague, poorly understood beyond local departmental staff, and did not necessarily take advantage of technology options that have emerged since inception of that process and quite often involved a substantial duplication of effort.

The main thrust of the Identity Management project is an initiative towards a goal of true interoperability between both learning and business systems. It is clear that duplication of effort and poorly defined process are inefficiencies in a sector that cannot afford to carry wasted resource from both people and technology resource perspectives. The intention with this project, actually a sequence of linked projects, was to make the business process more efficient and more visible through the pertinent use of technology.

In what context did we present this approach?- College Overview

Blackpool and The Fylde College is recognised as one of the top colleges in the country. It has been designated as a National Beacon of Excellence and was recently re-accredited for the Charter Mark in recognition of the excellent service it provides to all its learners. With an extensive provision covering a wide range of diverse areas of study including Maritime and Nautical Studies at the Fleetwood Campus. The College is the fourth largest FE provider of HE in the country, offering more than 80 qualifications in both contemporary and more traditional subjects, from diplomas to post-graduate programmes. As an Associate College of Lancaster University our degrees meet the rigorous requirements of the University. Blackpool and The Fylde College is one of the leaders in the North West in delivering Train to Gain across most sectors.

As long-term investment continues to create a sustainable future for Blackpool, the College has embarked upon a transformation programme of its own to provide vastly improved facilities for the community it serves.

Governance

The College, operating a mature and well structured management team maintains IT governance based on two major cross College committees known as eSystems and eLT Strategy with attendees that include both Vice Principals. Whereas there is often a succession of requests for providing new IT systems to enhance business process on an individual departmental basis, these on occasion can be rather limited to focusing on the relevance within any individual department. When a specific solution to a particular requirement emerges, the College will enthusiastically move forward to support a chosen methodology, but on occasion only really looking at an end point defined by a specific requirement. Identity Management requires a directive to look at moving the use of IT forward in a way that is for the benefit of the business as a whole. In this scenario ownership of such a project is maintained by the IT department. The systems approach to IT governance and decision making is based in the cross-college eSystems committee, chaired by the Vice Principal of Resources & Planning, Ruth Paisley, with attendance from key senior managers who participate in discussion and decision on the best use of information technology. It is at this forum that agreement to move forward with IDM based technologies was, and continues to be, made.

Stakeholders associated with the project were identified on a phased basis as the design was assessed and completed. Permanent stakeholders were colleagues within the IT support unit known then as College Network Services – Simon Bailey (Network Manager), Ken Eccles (Senior Network Engineer) and John Nicholson (Systems Development Engineer).

A significant advantage for the institution as a whole was that an IT department existed that already possessed that wider business vision. We found we could introduce the idea of Identity Management as a credible fix for a specific requirement, but then subsequently and rapidly reintroduce it again to satisfy a further requirement, and in doing so high lighting that by reusing this same approach we were getting better value from any previous original investments in time and man power.

How was this addressed previously?

Given the rather compartmentalised, or more specifically departmentalised, approach to identifying and addressing IT requirements, the development of technology based solutions was very much founded on a specific solution to a specific requirement. Typically, both the databases that contain key College business information and the technology solutions to enhance learning, were only ever connected on specific as-needs requirements. So, should any given database need to rely on a set of user records it would perhaps receive a batched, and possibly even just occasional, import of data from an appropriately selected source. This is very much a system-by-system approach rather than anything even moving towards a holistic methodology. Whilst almost always achieving an immediate objective, there was rarely a consideration for future needs. The duplication of effort and emerging disparity of transferred data was becoming an increasing burden for both data owners (application administrators) and the maintainers of the technology, and was quickly leading to situations where information could not be properly audited and data was slowly falling into disrepair, containing inconsistencies that could only be corrected on a local and occasional basis.

Problems

The challenge for the IT team was to break this short term cycle of accumulating disparate individually-linked databases and provide a system based entirely on *authoritative* data. We had to present this as a meaningful solution in the context of whole college business process without overwhelming busy college managers with technological detail, and also justifying a relatively large budget with demonstrable return of investment. When historically the organisation had succeeded in fulfilling the more short term specific needs why even consider a solution that is many times more complex and likely to take longer to fulfil? The key, obviously , is to look beyond the short term, properly cost consider the largely invisible wasted efforts associated with a "quick fix" and then review the real cost of a whole systems approach.

Presenting a project like this, without a laborious and detailed description that is likely to be received as a "technology rant", was a challenge. It was important to outline a larger future based on true interoperability and the efficiencies implicit in such an approach.

Technologies

For this institution, our key business systems are based on Oracle relational databases. Focussing on just the core business systems we see a Student Record System (SRS) built on Oracle, a Personnel HR database again built on an Oracle instance and a student VLE based on MySQL. A mature and reliable authentication domain based on Novell eDirectory has for well over a decade provided controlled and secured resource access to both staff and students. Many other systems, largely databases, built on Microsoft SQL and even including Microsoft Access, also participate in maintaining and reporting on business process. Relating back to the wide provision of education the College offers, we see some complex relationships on how data should present in the ideal world of efficient and effective IT delivery. Clearly, as is rarely the case, there was no possibility of a clean start and our approach relied on using the major advantages and benefits associated with incumbent technologies. Whilst the Novell eDirectory instance has performed almost flawlessly for many years, we were also required to address and support applications (including, most notably, the Student

Record System) that had moved to use a Microsoft Active Directory authentication model. What we were looking for was the “business glue” to reliably, yet flexibly, bond data services together from an identity driven perspective based on business rules. It was also particularly important that any such solution needed to be *event driven* rather than based on an occasional point-to-point system update. Naturally, when a suitable product emerged from Novell, we were receptively positioned to explore the offering whilst also being able to take advantage of keen academic pricing. Above all, and undeniably key to the interoperability agenda itself, it was very clear that this solution was platform agnostic. There was no requirement to use other Novell technologies, and the product itself was inclusive of many other vendors technology by design. It is perhaps unfortunate that the brand name of Novell often conjures up images of a provider of a now end of life operating system (Netware), that whilst providing remarkably efficient file and print services, is no longer a major market player. Undoubtedly some rather overwhelming technology options have emerged from the biggest players fronted by powerful marketing, but at the same time several developments from Novell, largely as the result of innovative acquisitions, have brought forward products that embrace and bind technologies from disparate manufacturers. Looking at the core product of Novell Identity Management we can see that modular product functionality is specifically offered for both Oracle and Microsoft technology solutions and in no way as an afterthought – bridging the key technology players in the current marketplace. This, in our opinion, would allow us to position the product right at the centre of key business systems.

How has FSD been designed?

The project was broken down into a number of phases to allow for a staged progression, and in doing so, provided an achievable map with demonstrable deliverables to maintain buy-in from stakeholders. Further phased development was very much anticipated at the start.Capital funding was identified to purchase the required software and a consideration made to justify a first process-driven engagement. Clearly, with an identity driven model for establishing interoperability, we needed to capture the two groups of user identities - staff and students. Given that this was the beginning of what promised to be a quite significant project, we looked for a least problematic requirement with soonest and most obvious return of investment. We needed a start point. Whereas it would be easy to imagine that linking student account management to an identity managed provision would bring some potentially very significant rewards, we already possessed a network account system that was loosely coupled to the Student Record System. A further, and very significant, potential advantage to the option of progressing a solution that established account provisioning services for staff was that the Human Resources department had recently auditioned and selected a replacement Personnel and Payroll management system, and were faced with the task of a thorough data cleanse exercise moving to this new system. We, as an IT department, were already aware that issues existed in relating live network account access to actual individuals who may no longer be in the employment of the College. Rationalising the HR department records to our own was a task that needed to be carried out and it therefore seemed an ideal opportunity to establish a tight link to this revised system.

Key Personnel

Key personnel for the project had to be found from the current staffing structure and indeed from staff that were already covering the support of an established and complex IT infrastructure. There would clearly be contention in respect of meeting day-to-day requirements and supporting a major project of this magnitude. However, as the staff concerned had already bought in to the concept of interoperability to realise a validated and more efficient IT environment, there quickly emerged a visible enthusiasm and commitment to take this forward. The size of the task with predicted futures was clearly an undertaking that could not be done lightly. The gains associated with true business-level interoperability were very attractive, but also required a very substantial commitment in the medium and longer terms. Historically, IT-centred projects were more typically based on immediate or short term gains with a far smaller investment in engineering time. It would be necessary to devote engineering resource and dynamically allocate other support requirements as immediate circumstance would undoubtedly dictate.

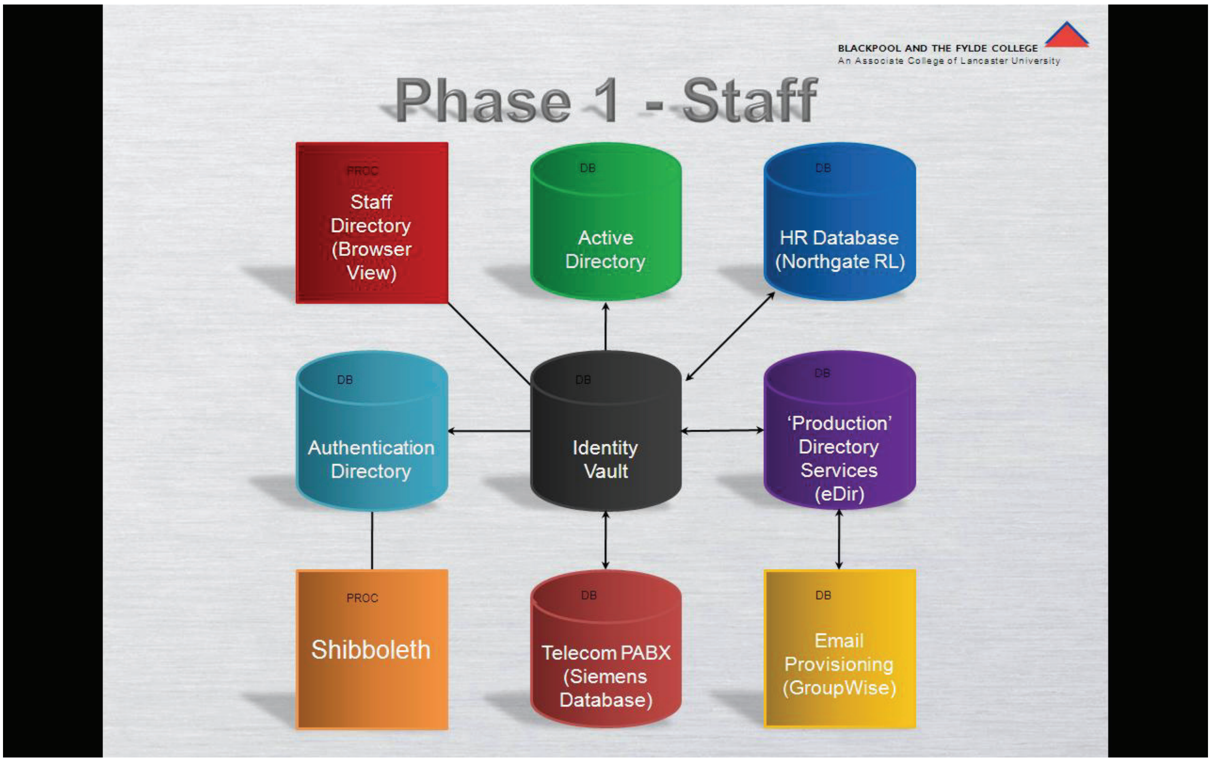
Training was available that was bespoke to the Novell Identity Management software suite and both key engineering staff were availed of a five day intensive course that was directly linked to typical objectives and allowed hands on access with using provided tools.

A key aspect to getting a good dependable build was initial design, and it was considered that at least in a first phase we should engage the services of an appropriately experienced IDM design specialist. As the technology was a new approach being underpinned by a solution designed and marketed by Novell, consultancy services were becoming available and from a known technology partner that had worked with the college for over a decade. First contact with the consultancy services confirmed availability but with a service that was more aligned to taking a collection of interoperability goals and developing a solution from start to finish. As an IT team, it was felt that we wanted greater ownership of any such project that we could further development in a time scale to match as yet unspecified, yet predictable, demands. The first steps, however, were also defining steps and some guidance to set off on the right path was definitely a reassuring benefit. Further dialogue with consultancy services saw the College commit to a relationship with the design partner to assist us to identify a correct design process and method to build this ourselves. The emphasis of this support was very much on design practice rather than mastering the required technology. This engagement proved very much fit for our purpose and pump-primed an identity driven model that progressed through subsequent years.

Implementation

The first two phases were enacted almost entirely asynchronously and first approached the maintenance of staff user accounts, based on interoperability with other key systems. The second phase moved over to focus on student accounts. Subsequent phases then went on to bind the two original phases together consolidating the pool of consolidated data and extending the reach to what were unconnected systems.

Phase 1



BLACKPOOL AND THE FYLDE COLLEGE
An Associate College of Lancaster University

Phase 1 - Staff

PROC
Staff Directory (Browser View)

DB
Active Directory

DB
HR Database (Northgate RL)

DB
Authentication Directory

DB
Identity Vault

DB
'Production' Directory Services (eDir)

PROC
Shibboleth

DB
Telecom PABX (Siemens Database)

DB
Email Provisioning (GroupWise)

Based on authoritative data about staff, that for legal purpose is required to reside on the Human Resource database, this information is extracted and presented to the "Identity Vault". The vault is a purpose built directory instance that stores the core data that is provisioned into connected systems. Each record is maintained and validated by a unique identifier. The information from the vault is presented to the following business systems –

i) The production directory for account access – the directory-controlled access to network services granting rights to applications, file storage and directory privilege.

ii) Tied to i), the same information is provided to the email system to generate, enable and disable email accounts.

iii) The Siemens telephone directory service – the directory , with browser based lookup, where information deemed authoritative is generated against incoming records from the HR system but via the vault. The telephone number is then provisioned into the HR system via the vault.

iv) An instance of Active Directory – information from the vault is provisioned into Active Directory to allow access to Microsoft technology based applications such as the Student Record System.

v) The information is made available via a web browser presented in the form of a staff directory. Staff members can browse key details about other staff, including working locations and telephone numbers (c/o the Siemens database).

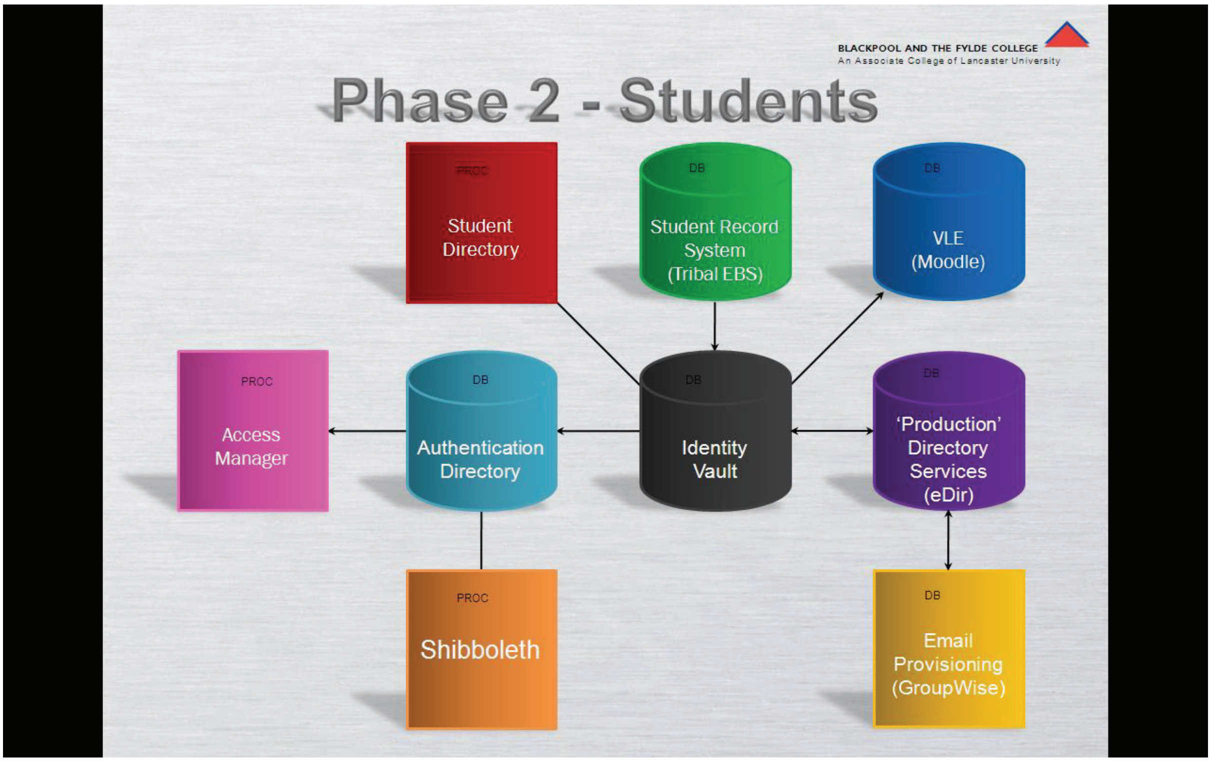
vi) Information is synchronised into an authentication database to provide a point of Single Sign On to a variety of web based applications.

At this point, and in order to kick-off the first phase, we needed to get a commitment from the HR department, as it would require a closer working relationship than had been previously established. We were fortunate to engage with the Deputy Director of Personnel who had the foresight to accept that this approach, with the interoperability benefits that it promised, would be a major benefit to the College as a whole. He also realised that by establishing a permanent link to other connected systems his data would have the greatest chance of remaining accurate and valid, having been coupled to other processes that would assist in rationalising any emerging disparities.

To push forward to a system design, we began to look at the core data we needed to get best functional value from a formal link between this new database and the rest of the business.

Subsequent phases of the identity based interoperability model would attempt to mirror both the design and development processes with varying levels of success.

Phase 2



BLACKPOOL AND THE FYLDE COLLEGE
An Associate College of Lancaster University

Phase 2 - Students

Some 2 years later, and after an extensive planning cycle containing seemingly unavoidable delays, we collectively moved to harvesting and maintaining details from the Student Record System. The authoritative home for student data is clearly within a student records provision and includes information that is absolutely key to the user experience during their time at college. We would seek to use selected aspects of this information to enhance data provision within connected applications and took particular focus on the Virtual Learning Environment. An outline of this second phase is as follows :-

i) At enrolment time, the information is input to the Student Record System, recording detail such as course code and campus.

ii) The vault provisions this information into the Moodle MYSQL database, providing a directly accessible link to the learner number, referenced to the course record, as generated by the course database.

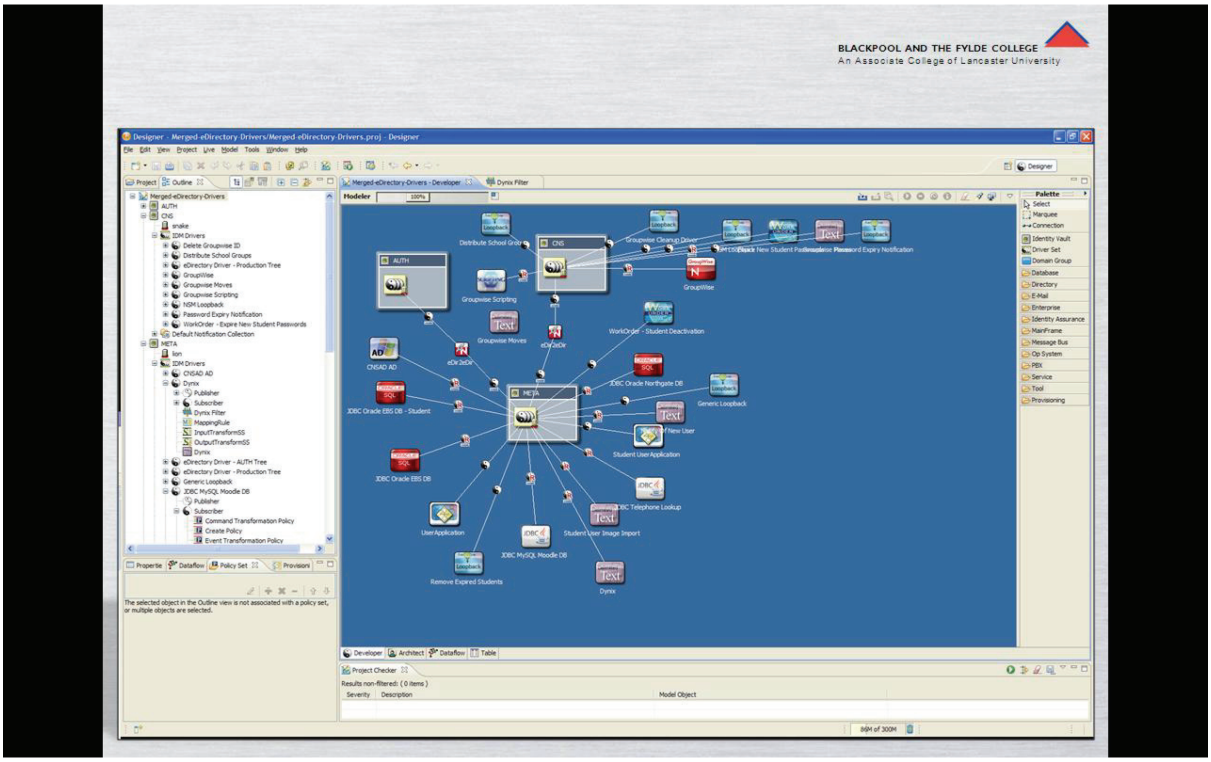
iii) The vault provisions information into the production directory to generate and maintain student account information.

iv) The production directory, driven by information from the vault, is used to provision email accounts.

v) A browsable interface is made available to allow selective access to individual record properties, such as mobile phone number and emergency contact details, to allow students to amend their information as desired.

vi) The information is synchronised into an authentication database providing Single Sign On to learning materials, but also allowing for Shibboleth authentication to global information systems.

The Novell technology based Identity Management solution is supported by a tool that provides a logical view of the interoperability relationships within a business system, based on the full extent of any project at any given point in time. The snapshot below shows project progression with key system connection relationships.



The selected object in the Outline view is not associated with a policy set, or multiple objects are selected.

Results non-filtered: (0 items)

Whereas there is an immense amount of detail contained therein, the architecture is logical and infinitely flexible and therefore lends itself to defining the relationships between business systems.

The Ying-Yang symbols are the locations of rules that describe data interchange, based on agreed business rules. The technology has been designed to be flexible enough to meet complex rule-based requirements. A further benefit is that the software can "self-document" providing a template of inputs versus outputs that is presented in a plain-English format, and can therefore be consumed by non-technical staff.

The key sell of identity management for participating departments within any particular phase is the potential to improve and enhance business process within that same department. Traditionally, when a new IT based service emerges, it is more usually considered as a potential additional burden, albeit with new functional benefits. It is generally a hard sell to countenance support from departmental staff that would almost certainly consider they have enough to occupy their working hours. The sell, directed to managerial staff responsible for overall department function, is that there may be some tangible benefits to re-looking at the way business process is conducted and so demonstrate improvements to the business as a whole, but in so doing not generate additional work (and possibly even reduce existing workload). As soon as tangible benefits to any given department can be demonstrated, you have the required buy-in to proceed.

Another milestone in promoting this approach was a live demonstration of how automated account provisioning and control actually occurs in real time. This was presented to the colleges eSystems committee and in a manner that was very visual and very much accessible to non-technical staff who have a very keen interest in improving business process. The demonstration proved highly effective and most notably got the positive attentions of the Director of Finance and Vice Principals who could see not only the immediate benefits but also how powerful connected systems could be.

Given that part of the implementation process was based in an entirely separate test environment, it was possible to run a simulated trial of a design model and henceforth reduce the risk associated with ambiguities at technical or operational levels. The scoped-out project was assembled using a direct clone of the live systems and "real operators" brought in to experience and examine results. This singularly most important test process was conducted meticulously around a formally drawn up testing plan to measure input against output and look for any deviation from identified and agreed business process.

Once the testing procedures were completed, we were in a position to agree a go-live date that suited all parties. The date was set to avoid calendar hot-spots and also to allow for contingency engineering time to pick up any emerging issues. In reality, no immediate surprises were expected and nothing presented. The main source of problem issues were associated with divergence from defined business process. Sometimes this deviation was a disadvantage (i.e. bad practice)to the business but at other times exceptions would present that were valid, and could be detrimental if not acted upon. Of course, with a clearly designed set of business rules this represents a problem, and some minor reworks, particularly associated with the second phase, were necessary to maintain output. On the whole, and based on agreed core operating requirements, the system was highly effective and problem free – as validated by the stakeholders.

<u>Benefits – a brief synopsis of the benefits of this FSD approach</u>

Once the project modelling was complete and able to provide a clear business process, it was relatively easy to assess and publicise benefits.

The key benefits of phase one are –

i) Zero-day start for staff, such that as soon as a start date is provisioned by Human Resource they have immediate network access.

ii) Zero-day finish, so that when an employment is terminated, the account access is automatically removed on the final date of paid employment.

iii) Access to an email account.

iv) The processes-controlled allocation of telephone numbers.

v) Browsable lookup of staff details and phone numbers.

vi) Global access to web based application via a Single Sign On password.

The key benefits of phase two are –

i) Real-time provisioning of network accounts, based on verified and validated information from the Student Record System.

ii) Access to an email account.

iii) Selective availability of an account within the Moodle based Virtual Learning Environment, indexed by course-code designation.

iv) Shibboleth authentication to remote learning materials based on validated enrolled identities.

v) The ability to update contact information within a browser based interface.

Almost every functional aspect of a successfully designed identity managed project should be able to display an improvement and, at least, a greater clarity of actual business process. If any specific benefit applies to the wider business i.e. beyond “departmental walls” it is quite often very visible as a service improvement from the department that is being “process enhanced” to others. The majority of staff who may only be associated with the task of data entry should still be able to see that the function they perform is going to better use, for both the department and the business as a whole, if that communication is effective .

The FSD "Pilot" phase – Phases 2.5, Phase 3 & Phase 4 (in development)

Further development of the IDM project with funding assistance from the JISC FSD "Pilot" initiative enabled progression into three additional key system areas that had been considered during previous phases. The three areas we identified were Apple Mac integration, integration of the College Library Management System (LMS) and management of a "cloud based" email, application and storage solution.

IDM 2.5

The first extension of existing services was based on joining the functionality of the two previous phases allowing us to complete the identity management of staff in the context of the (authoritative) student record database. Whereas we had previously identified authoritative data on staff credentials from the Personnel database and provisioned these to our central vault, there is an application that looks directly at the student record database for staff information. Clearly this information must be sourced from the vault but previous to this exercise a manual process of writing individual records in to the student database had been necessary. This approach was flawed and a good deal of inaccurate or duplicated data became evident. Once again we are looking at a data cleanse exercise to remove any mismatched manually input records so that any incoming authoritative data from the vault would match and not cause further duplication. The exercise took several passes through the data and highlighted a number of protocol / syntax issues - inconsistencies with so called double-barrelled surnames where a bug in the HR database would disallow Firstname Surname-Surname capitalisation which quite naturally would be seen as syntactically correct. It was a little difficult to impart the importance of the exacting data format required. Notably, the data we were trying to cleanse, which included data that was input many years earlier and that predated the creation of the newer HR database, and was therefore orphaned. An example of this was members of staff that had left employment of the College over five years ago but had their legacy data entries in the student record system. In this intermediate phase;

- Write staff and student data into the SRS - Tribal EBS.
- Create staff members within EBS as they are processed within the Northgate Personnel system
- Update student attributes through self service (not yet made available but implemented)
- Majority of users already manually input - required substantial data cleanse
    - No consistent unique ID linking data between the systems, including; missing, incorrect, old format workforce Ids, inconsistent spelling of identifying data, lack of national insurance information, etc.
    - Unlike the Personnel integration, legacy and unmaintained staff information still existed from years earlier e.g. staff that have left the institution several years ago
- Create Business Procedure to cope with a new member of staff already existing within the EBS Student Record system (e.g. Current and ex-students or staff). Because there is no guaranteed unique identifier between a new record within Northgate and an *existing* record within EBS, we needed manual intervention to ensure reliable matching. On an event where a staff record is not matched, an e-mail is sent to a member of MI&F who will perform the matching process which if successful they can enter the Workforce ID to permit the match. If

no match is found they are able to instruct the IDM system to create a new staff record within EBS.

- Pressure to complete the task to facilitate access to third party web app designed to expose key data about students – mission critical.
- Reporting mechanism where “critical” properties changed within EBS are “reset” by the Authoritative data source are sent to members of the MI&F team, so they can verify which version of the information is correct. Improves data accuracy by flagging changes that are being attempted while retaining the authority of the source system.
- The triggers are actually more simple than the student related ones.
- Staff photos procedure to enable a mechanism for the production of Staff Badges.

The purpose and benefits of this intermediate phase, which essentially bridges and completes phases 1 and 2 is that it very clearly presents the same authoritative data to what is arguably the most significant IT database at the College. The real challenge that presented was that the organisation was requiring to present data via a system that had been populated with data that in this new context was not sanitised for this same purpose. When the SRS was originally populated and the data therein moderated at input there was no expectation that the data might at some future time be used in the way that certain third party applications would wish to use and expose. The data cleanse was absolutely necessary but the predicament where this same dirty data was assumed to be redundant, but was later to be exposed, whilst now functionally disadvantageous could not have reasonably been predicted. Although the desired outcome was clear the process was labour intensive and a burden to enact.

Phase 3 a - Apple Mac integration

A situation existed where staff and student accounts were created using a time consuming manual import process each year for students within the specific Art and Design department who predominantly worked with Apple Mac workstations. They already had credentials to use the majority PC based network but these were not recognised on this linked but separate sub-network. This resulted in only Art & Design students being able to use Apple workstations and required Art & Design students to memorise and use two or three sets of account credentials. The credentials of the vast majority of students were therefore unrecognised by this local domain. As there was no link between the Mac system and the general central system , either batched or fully dynamic password synch issues between Apple based login and GroupWise mail systems was a continuing significant issue. As users were obliged to manually keep their passwords matched, this was causing confusion particularly when other systems were functioning with Single Sign On. A very similar problem scenario was also evident in that two Open Directories were in operation for the two sites (University Centre & Park Road) producing a lack of consistency between the two sites so in a worse case situation students were operating on three separate network facilities whilst needing to access common resources such as email and Internet with another password. Whilst workable there was a great deal of direct support required to maintain service availability and it was clear to users that they had a system that was in part disadvantaged.

The targets of the identity management objective were therefore –

1. For all staff and students to be able to use Mac workstations.
2. To have consistent credentials across all sites and systems.
3. More simplified password management.
4. Password synchronisation.
5. Automated account deployment and revocation.
6. Single sign-on retention for Mac systems.

This was a particularly complex scenario and although accepted (nothing else better had ever existed) was a compromised and very loosely managed user database that was not strictly identity managed. The problem scenario was clearly very much technically set within directory support and therefore well suited to deployment using previously gained expertise and related solutions.

We initially investigated the following approaches:

- Open directory
  - Could synchronise into the directory for Mac authentication but couldn’t password synch bi directionally
- eDirectory + Kerberos
  - Old, outdated Kerberos implementation making it difficult to implement and maintain. Concern on future support also.
- eDirectory / LDAP
  - Loss of single signon
- AD

    - Proved to be the most successful implementation. While still using Open Directory for Mac configuration that is local to the site, the AD is used for all authentication and single signon activity meaning that only one credential repository needs to be kept up to date. We are then able to bi-directionally synch between IDM Vault and MAC-AD required attributes including passwords for centralised password management.
- A Windows 2008 AD Domain controller used for our implementation
- Password synchronisation enacted

The middle-ware directory provision hosted by Active Directory very much proved to be the solution of choice. An interesting scenario where the eDirectory vault initially native to Novell technologies goes via the pure Microsoft directory solution (limited to run only on Windows hosts) to enable authentication with Apple Macintosh clients – quite a hybrid mix but a functionally effective one that since launch has proved immensely beneficial to both staff and students using the extensive Apple Mac facility.

Phase 3b – Library Management System (LMS)

Perhaps in some ways ironically our IDM journey was originally set to begin with the management of users in our own Library Management System. When we first took a look at removing what was a particularly striking example of data duplication, where data was having to be re-keyed for a specific purpose, significant obstacles presented. The main issue was that the application solution provider was unwilling to lend support to our purpose and their application was essentially limited to their proprietary needs. Newer versions of the application were emerging – but at a very significant cost.

The solution proceeded with highlights as follows:-

- Horizon LMS (and previous Dynix) systems that were populated using imported data that presented a great deal of legacy data.
    - The incumbent LMS had been used for over a decade and during this time various upgrades had been performed dragging data between developing application functionality. Whilst such development was suitable to the organisations need it did result in an accumulation of dirty data.
- No support whatsoever from application vendor (due to no commercial gain) – provided only with primitive Import tools that were not developed with this purpose.
- Very minimal documentation of bimport tool.
- The database had initially been installed to operate on the wrong port.
- Use of IDM "Text driver" to format data to meet the expectations of Import utility.
- Part of the solution required that a Java driver shim had to be written to create headings for csv file.
- No definitive matching criteria – c/o extensive amount of legacy data
- Duplicate records with no unique identifier in common
- Applications need to use "second_id" field in order to search within GUI
- Define a "borrower type" not possible with current data – (HE v FE) so a custom script written to interrogate the database so entries were not overwritten on initial sync.

What could essentially have been a relatively technologically simple requirement was made far more complex by operational constraints and difficult to cleanse data. It took a year for the administrators of the application to be able to get a to a position where the data could be rationalised without functional process disadvantage. Academic year 2011/12 is expected to use authoritative data from the College SMS.

Phase 3c - Google v Live@Edu

This aspect of the development had unfortunately been delayed due to uncertainties within the organisation on which “cloud based” service we should adopt. There exist two quite distinct services presented by the global IT presences of Google and Microsoft – Google Apps and Live@Edu respectively. Each has its own merit but essentially the services exist to provide a hosted environment to access individual user data with a selection of web applications. Uptake of these services has been significant within the sector and it is clear this is something more than a trend. Many universities moved to support and typically recommend Google Apps for just students (though on occasion staff also) and were thus required to link these out-sourced accounts to their internal student record system and other internal IT resource.

The issue we have had is that a decision based on identifying the best suited of the alternatives had not been taken. Clearly we had not wished to influence or rush such an important decision and had therefore been obliged to put this aspect of the development delivery temporarily on hold. We had however already examined the feasibility of moving this forward by examining what other institutions have already achieved and what pre-existing tools there are available already.

The key aspects of this phase were:-

- Set up test domain of staff.blackpool.ac.uk for email and applications.
- Investigated the use of Google apps directory sync utility.
- Investigated the use of Novell IDM – custom java based driver would be needed such as the ‘Cosmo-key’ driver utility.
- No strategic management decision (at that time) on a possible move to a Microsoft based infrastructure including (assumed) Live@Edu stopped commencement the technical build.
- “Student parliaments” held to assess need/usefulness of Google apps or MS Live@Edu gave a mixed response.
- A decision was taken to move forward early in 2011 for students with Live@Edu to be available in September 2011.
- As a result of specific further developments from Google the decision was reversed and a strategic decision made to engage with Google Apps to be offered as an option to students only.
- Available driver tool sets were again re-evaluated and a very clear favoured tool identified that was supported by, but not written by, Novell was identified and purchased mid 2011.

The more recent development that shone through from Google was a very determined and worthwhile module to enable integration with the Moodle Virtual Learning Environment. This valuable eLearning tool has been in use at the College for many years and is a much used platform by staff and students. Further development of Moodle as a resource is ongoing and the organisation has made a wise and determined commitment to encourage use of this very popular Virtual Learning Environment. The decision to standardise on Google Apps means that our investment of resource and efforts are well directed to close integration with our IDM estate such that student learner accounts are provisioned out to the Google Apps cloud. The driver set purchased (from JISC Pilot funding) enables us to establish a reliable and third party maintained driver solution taking full advantage of the pre-existing IDM estate. For this institution this releases yet more value for money on the initial and continuing investment in its entirety, but it is our belief that other sites are adopting an IDM approach based on the need to synchronise to Google Apps as a sole directive.

Phase 3 additional application - MELD

The College has very specific requirements to monitor the quality of provision offered and to this affect supports a Quality & Standards department charged with assessing and monitoring the delivery of learning and associated practices. Such required targets are mandatory and regulated by external authorities including funding bodies. Applications to record some of this departments requirements are relatively few and tend to be internal developments by other institutions based on standard office software such as Microsoft SQL or even just customised extensions' of Microsoft Office. The Quality & Standards department had already identified a suitable tool for their purpose in the form of an application called MELD. Built around a relatively straight forward MS SQL instance the application was developed for a specific purpose by a single developer in another college. When Q & S adopted the software the scope was limited to a handful of employees which could be easily managed by manual input duplicating detail from existing records. Moving out of this limited pilot phase it quickly became evident that all staff should reasonably be expected to participate either by submission or simply to be able to be able to view quality procedures in progress. The quite unexpected requirement to produce an up-scaled deployment to include all College staff users proceeded as follows:-

Requirements.

- A sudden and urgent requirement to extend a limited application – a clear requirement.
- SQL Server database application – the program was functionally understood.
- Buy in from the application developer – direct contact explaining our reasoned requirements got full support from the owner of the software application.
- Documentation with explanation of how to create new users.
- Very little legacy data as only previously rolled out to a handful of staff – this still needed taking into account during the matching process.
- Consideration for the implications of users changing the data/deleting users from within the administration console of the application.

Options.

- 2 possible approaches –

    - 1. To enter data directly into the tables – proved unworkable as too many tables needed updating and data needed sorting into a specific order after it had been inserted.
    - 2. Create staging table and apply custom triggers combined with stored procedures to manipulate the data

Outcome

- Option 2 selected as immediately practicable.
- Extensive logging to database table of all changes.

The solution was delivered in a very timely manner and was deemed fit for purpose by the Quality & Standards department. Our local development was fed back to the application author such that future updates of the application may be delivered without issue to our bespoke work. The way the solution was developed very much minimises the chance of future incompatibly. The College appreciates the support provided by the developer of the MELD application which very much assisted in the timely deployment of this solution.

Continual maintenance of phase 2

As the team progressed into further system interoperability, and in so doing accumulating experience in extending the IDM solution, there were occasions when minor modifications to the function of phases previously deemed complete became necessary and appropriate. Typically such modifications were based on exceptional circumstances where the use of data was non-typical but still valid. As the entire solution is modular in nature and to a large degree is self documenting this rarely proved to be an arduous task. Specifically we found some examples in phase 2 where triggers weren't delivering 100% accurate student and enrolment data. Improvements were therefore necessary as problems were only exposed using various methods of data validity checking. Work is ongoing but, most importantly, significantly improves the quality of data being committed to the database.

Data cleanse

Throughout all phases of the Identity Management development project and its constituent parts we have found the requirement to clean legacy data to be one of the most significant and arduous challenges for our project associates. On occasion it seemed that the consequences of over a decade of accumulated manually input data seemed not to be understood till 'go live' on any given phase. The stepped change to attach to an authoritative data source and the uncompromised nature that the enhanced service provides forces discipline to make the rigid input of data a requirement. The culture whereby data input rules are conveniently manipulated to achieve a specific and sometimes urgent objective prevails in some business areas. First impressions are that the "tail is wagging the dog" and that process is being somehow compromised by the new service. Restoring the vision normally restores both belief and commitment. Certain phases were delayed when the original data was discovered to have some continuing value linked to, but not central to, the requirement being managed. An example of this was where in the data relating to the Library Management System the requirement to maintain a log of overdue returns fines that may still apply to both current students and students that are no longer enrolled on any course. Whilst not representing any specific requirement of the sub-project brief it did quite suddenly present as a substantial obstacle. It is reasonable to say that the re-evaluation of the process function is worthwhile in its own right and that the implicit tie to authoritative data that is created is of immense value in both the present and future. It is however pleasing and highly significant to note that although deficiencies in data which have on occasion seriously delayed project objectives, that the associated necessary remedial works direct department local activity to a far more holistic business solution. An example, still to be resolved, and looking way back to the first phase of the project integrating Personnel information with a new database (Northgate RL), we see areas concerning where the input of additional data would have been highly beneficial and thus based on this far more holistic strategy. It is highly notable that there is a distinct shift in culture when considering embarking on new IT projects. A willingness to look at overall benefits in the context of more immediate business requirements is increasingly prevalent.

Evaluation & re-evaluation

The project has been evaluated throughout by stakeholders and, once deployed on live systems, becomes an ongoing live business process. Deviation from expected results are reported to project team members directly, who are required to continually evaluate any deviation from an ideal predicted outcome.

Entire process phases were brought forward in outline at various technology focus forums both internally and involving several other quite separate institutions – see later.

Disadvantages or drawbacks?

A good deal of the risks associated were assessed and managed within the test environment so as to significantly reduce any problems with deviation from true process.

After five plus years of sustained development, the return on investment, whilst based on a complex business model, is clear to those with an overall view of an Information Technology led business process. It is, however, this same complex model that is vulnerable to a less than comprehensive observation. Few members of staff or external bodies have been able to see the vision as a whole and there remains an opportunity where inappropriate assessment could miss the inherent value of the project in its far reaching entirety – both actual and potential. The continued challenge to communicate and market the purpose behind this approach is an ongoing task. Even recently we have discovered pockets of staff that, whilst aware of the "Identity Management Project", do not really comprehend the overall objective. Once the project, with its longer term objectives and suggested futures, are explained in an appropriate context, the vast majority of now enlightened staff are both impressed and convinced of its inherent merit. It is, however, a complex message that does well to be reiterated on occasion to preserve both the meaning and impetus to maintain policy associated with the project and assess and plan future expansions.

The other notable and occasionally recurrent issues, directs participants to focus on sign-off at key project milestones. Even after extensive and detailed discussion assembling and documenting what is desired business practice, there were instances when agreed outcomes were not quite that which was described by stakeholders. Most typically, variation from the "assumed" norm presented as exceptions but on one occasion, advice proffered did not turn out to follow actual process. Whilst undesirable, realistically it is necessary to be ready to address variance in a constructive way. Obtaining sign-off is a powerful way of getting committed responsibility.

IDM 2010

Whilst accumulating knowledge on current developments in IDM we became aware of a focused national event that recently came into existence and now occurs on an annual basis in London called IDM2010. The event is entirely focused on the Identity Management service and attracts vendors with IDM solutions (both actual software product and associated consultancy) targeting both public and private sectors. The original contact was based on an invitation to the author to present at the event as one of four public sector showcases. Whilst this was indeed flattering it required a very considerable commitment to construct a professional presentation to a high profile audience. Prevailing conditions within the College were, regrettably, at odds with such a request. It has transpired that our work on the IDM project has circulated throughout the IT community and even the rather minimal content on our web site / blog is being seen.

We did however attend the event based on complimentary admission. The event was extremely popular and representatives from major global institutions such as Barclays Global, major sectors of the NHS and education sector were evident. It was interesting to see how this common drive to manage identities easily and enthusiastically attracted the interest and subsequent buy-in from such a diverse audience.

Perhaps one of the most gratifying discoveries was that amongst the product offerings exhibited it appeared that Novell's Identity Management platform was held in high regard sitting well against rival products from the like of IBM and Oracle. Our judgement call about the capability and futures for this product suite seem to have been shared by some very major players in both public and private sectors. Discussions with senior representatives from Novell and key third parties selling consultancy and build services for an Identity Managed environment underlined just how far we have progressed with an almost wholly internally delivered solution. It has become apparent that the discipline required to scope an identity managed project does, on occasion, result in compromise when that project is delivered by an external consultancy. We are aware that externally managed projects often appear to reduce scope down to minimal targets but that these targets are guaranteed to be achievable allowing for, and building out, potentially significant business process unknowns. As business process is often complex and flexible an external consultancy is likely to need to compromise process detail to a point where the process output is compromised also. Whereas we as internal employees of a company have detailed insight to business purpose and know where such process is conducted it is perhaps unrealistic to expect a visiting consulting entity to assimilate detail particularly when participants are spread throughout an organisation. Identification of process with composite elements to define responsibility, accountability associated with actual process is often a complex and time consuming endeavour. Typically the more personnel that are involved with process the higher the likelihood of the development of "micro-process" that whilst functionally valid are not clearly visible as a part of the business workflow yet must be taken into account to define and indeed legitimise a specific process requirement and function.

A tale of three institutions

During the course of the Pilot phase of the project we made a distinct effort to promote awareness of our work to other similar organisations we would have any contact with. The College is well known within the sector and necessarily encourages the sharing of good practice with similar institutions. During the life cycle of the Pilot phase contact was made with three specific institutions to explore whether they had an interest or need, declared or otherwise, in the management of user identities. Responses to a first contact varied immensely from complete non-recognition of the discipline to “oh yes, we already do that”.

Institution A

The first intuition we had contact were initially very comfortable that they had a solution in place that was essentially similar and it was very clear to see that there was a clear holistic drive to IT systems interoperability and a determination to efficiently manage business process as a whole. There was a very obvious maturity and structure to how they had arrived at their solution but they were still very enthusiastic to listen to the approach taken by Blackpool & the Fylde College. It was however interesting to note that that they made a stepped change in how their solution was delivered switching to a solution offered by a major industry IDM tool provider.

Institution B

A specific, and largely unrelated engagement, lead to an opportunity to speak directly with another college, and provided an opportunity to branch out into wider IT issues such as managing the user life cycle. It transpired that the management of the creation and removal of staff user accounts was a problem area that whilst not functionally detrimental was causing inefficiencies and demonstrable inconsistencies. A subsequent and dedicated day long focus session on the advantages of our approach to really pinning down the user account life cycle was well received and was very clearly thought provoking. We made a very determined effort to paint a realistic picture highlighting the very definite gains but also taking care to explain the possible pitfalls and difficulties that one might reasonably expect to experience. It is hoped, that unlike a manufacturer or reseller, as we have nothing to sell and therefore nothing to hide, our experience was trusted and validated.

Institution C

In no way related to either of the other consultation sessions came an opportunity to compare notes with a like minded college who were already well advanced with a not dissimilar approach to our own. Circumstances locally had unfortunately brought their development to a hiatus and specific problems with functionality had been significant enough to consider an option to entirely abandon the progress that had been made. At that time no better alternative had been identified and the decision was resting at an exploratory level. It was fairly clear from the outset that we had something to offer by way of a no cost objective and experienced overview of their specific issues and some constructive opinion based on hindsight. The commitment to move forward with an infrastructure based on rigid identity management is significant, and in circumstances where the solution fails to deliver or in a worst case instance actually potentially causes harm to business process, there is a quite reasonable tendency to consider drawing away from what could be a flawed solution. Joint analysis of their specific predicament quite quickly lead both parties to accept that the process being represented was “unsafe”. This is distinctly different to any possible failure in the technology. An option therefore exists that the process is revisited and re-engineered to be “safe”. It is our belief that the organisation has since engaged in this re-engineering process and intends to move forward with their identity managed estate having been suitably impressed by our own efforts at the College.

All three IDM related engagements gave us a direct opportunity to display and discuss what we believe is user life cycle management best practice but at the same time provided us with an opportunity to have our work critically appraised.

Phase 4 – in development

Although work is not yet completed in Phase 3c and the Google Apps driver needs to be configured, refined and tested, a further and quite dramatic functional use of process control through IDM has been identified and is moving swiftly through a design phase. Until this time identity management was limited to enrolled student learners and payroll staff. This next phase sees us push out the catchment net to incorporate and uniquely identify *potential* student customers.

The design brief is based on a requirement for the College to be able to uniquely identify and address prospective students such that at a very early stage of making a course application we could assign them access to appropriate resource including items such as outline course information. Once an application (i.e. a potential student has identified a course that they wish to apply for) has been uniquely logged we intend to generate a student record in the Student Record System (EBS) as is already the case for validated enrolments c/o phase 2. This project phase makes use of a web based module that is part of the SRS to allow potential students to enter their relevant credentials to enable the creation of a unique learner record but via a manual de-duplication process. The record would, ideally, be flagged as a valid enrolment when the enrolment instance is processed through to completion. It is important to remember that making what could be thought of as a segregated addition to the student life cycle process does actually necessitate a look again at that complete lifecycle.

Whilst this is a major addition involving quite different teams of student administrative staff it is potentially a very rewarding tool for the College to be able to use allowing the College to start a relationship with a prospective student at a very early stage.

Summary & Reflection

This now combined Pathfinder and Pilot case study seeks to capture over five years of development of system interoperability and in doing so represent the many tangible benefits that have become highlights. Perhaps the most gratifying experience has been working with staff at departmental level to enhance business process and in so doing developing efficiencies. To be able to present an IT project that suggests service improvement as a core ideal has been rewarding. At no stage in the project have we ever had occasion to doubt the true validity of the project, and the return on investment has grown throughout. At each additional phase we see greater value extracted from the previous phases as the groundwork is already in place.

An area that comes highly recommended, and that in itself would have assisted in meeting project deadlines, is good project management practice. The team that was engaged in the build previously had little experience of managing a project where involvement with multiple parties, such as internal and external customers, is an absolute necessity. Previous project experience was typically limited to just one or two entities and presented with a time line that was easily visible throughout. When there is an obligation to manage time between several parties at once, and also continue to be challenged by emerging base-infrastructure support requirements, delays and breaks emerge based on non-availability. The team, although able to deliver and meet deadlines, would have had a more comfortable time following agreed project milestones. Project management is highly recommended, if not an absolute necessity.

As the project has progressed and further entities are assessed for interoperability benefits, we continue to see additional return on investment but also a number of in some ways unanticipated benefits. One such benefit is the response from both internal and external auditors who approach college business systems in such a way that they are probing for examples of less than satisfactory business practice. Typically, auditors are hugely impressed with the outcomes of this project. Being able to demonstrate that data throughput involving operators is definitively mapped by authoritatively provisioned user accounts that are tied to systems driven by clear policy, provides clarity and authenticity to a process that is not reliant on a paper trail.

Engagement on a project of this wide-reaching nature undoubtedly represents a considerable amount of forward investment in both time and, to a lesser degree, budget, but when expectations are temporarily contained to an immediate set of required benefits to meet an immediate set of objectives, a degree of success can be demonstrated that can be built on. From a set of completed objectives there is then a template and a discipline to re-apply the approach as business needs will dictate.

Building on successes – as we considered and enacted extension, revision or creation of entirely new phases we adopt a practice where we pro-actively revisit customers that were assisted in a previous phase. This was in part to consider onward value of development but also to demonstrate assurance to newer participants.

Avoiding the pitfalls – based on previous experience with some of the data owners we determined to get comprehensive business logic upfront but did not always succeed. Realistically, working within an organisation that is obliged to respond to a wide spectrum of business requirements from a variety of bodies it is only reasonable to expect focus on any specific aspect of the project to temporarily recede. An awareness and ability to work around such instances is crucial but the very recognition of such a phenomena is a crucial aspect of working to a successful process recognition and solution.

To summarise, our experience suggests that it is a advantage to start small, produce deliverables that meet immediate business requirements, and then progress a well understood fundamentally inclusive discipline to incorporate other business systems, demonstrating increasing return of investment. As IT developments play an increasing significance in business function it is particularly important that such a core development be able to embrace changes of infrastructure. Of particular significance is a shift to a reliance on Microsoft technology solutions and an extension of the delivery of IT from the emerging cloud. Like many other leading institutions advantages of a Microsoft centric IT delivery offer a more seamless solution being a best fit for applications intended for such an anticipated environment.