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

- a JISC "Pathfinder" Project on four 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, but 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 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 pointing out 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 an as-needs basis. 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 appropriate 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.

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 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. 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 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 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.

Phase 1

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).

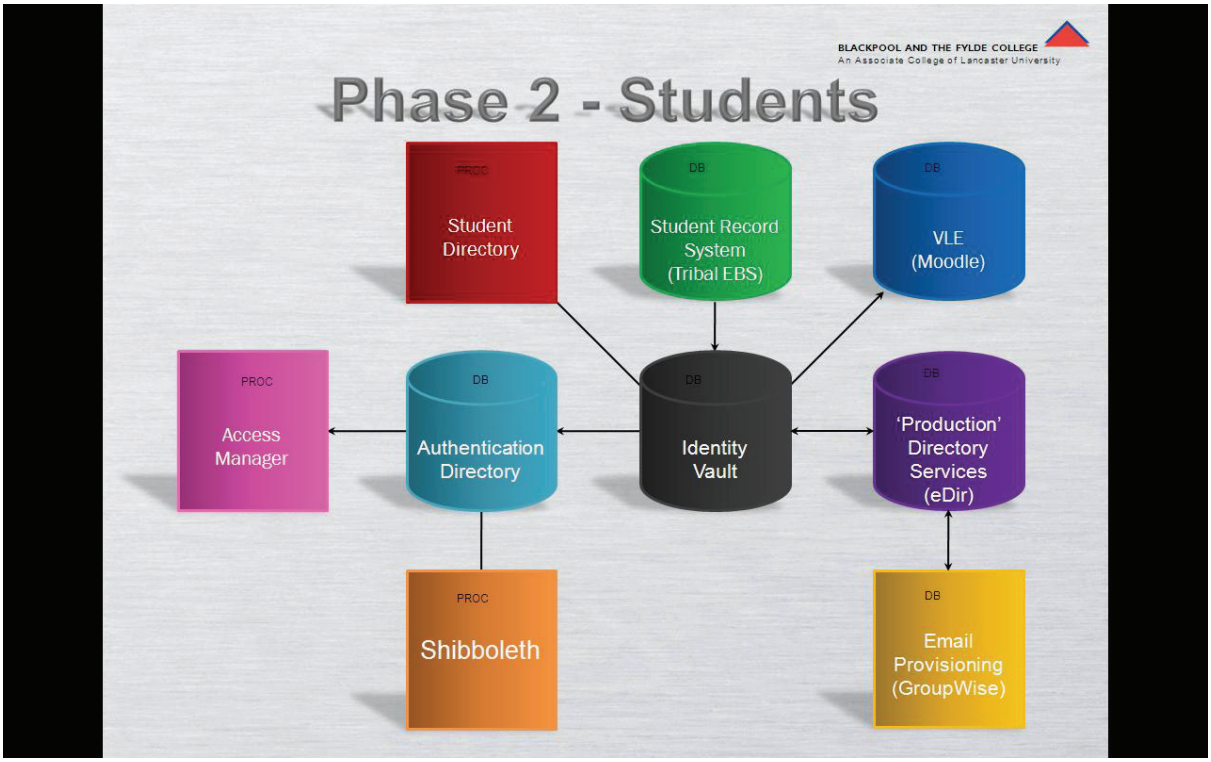
vi) Information is synchronised into an authentication database to provide a point of Single Sign On to a variety of web based applications.

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



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.

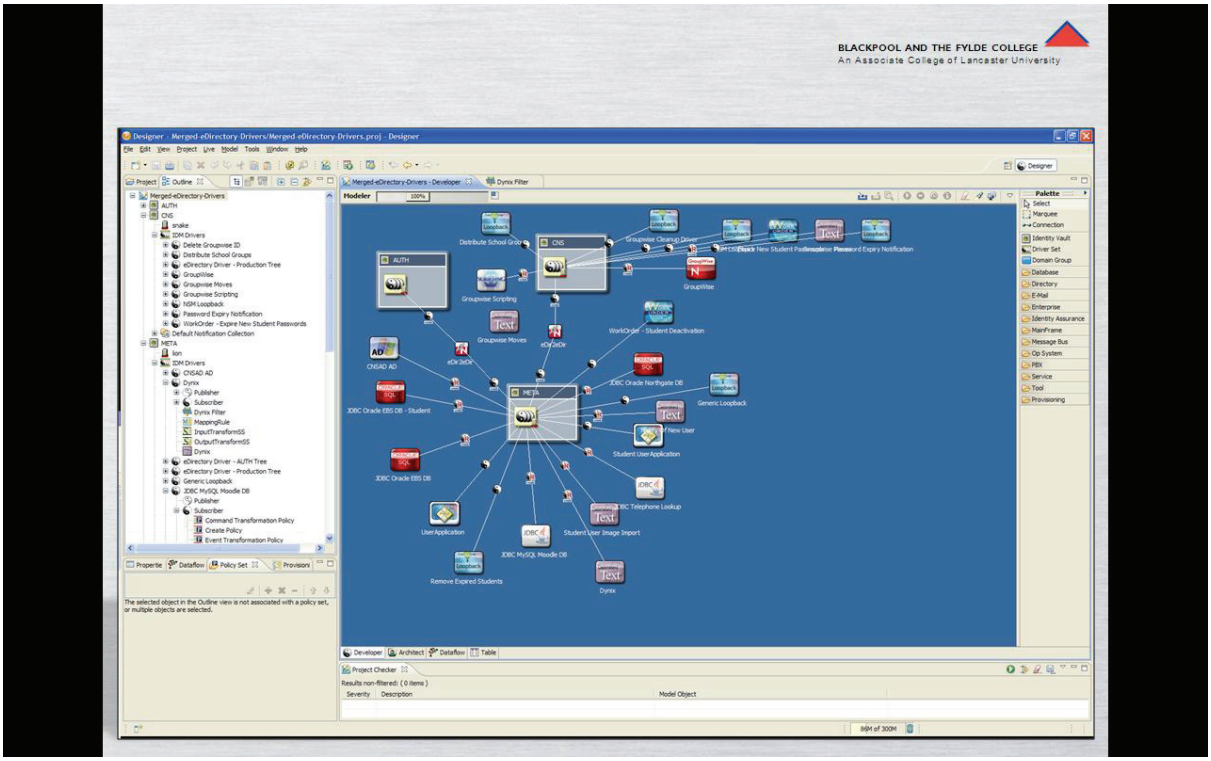
iii) The vault provisions information into the production directory to generate and maintain student account information.

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.



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 .

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.

Disadvantages or drawbacks? - Complexity versus communication

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 four years of sustained development, the return on investment, whilst based on a complex model, is clear to those with an overall view of an Information Technology led business process. It is, however, this 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 even begin to 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. It is, however, a complex message that needs to be reiterated on occasion to preserve both the meaning and impetus to maintain policy associated with the project and assess and plan future expansion.

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 what 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.

Progression beyond the first two phases

Given that development of futures surrounding information technology related projects are likely to encompass more and more aspects associated with the interoperability of data, not only within the institution, but extending into the emerging Cloud, it is easy to see that this project could and should grow way beyond the connected systems we have assembled in these past four years. We have already identified several future connections to internal and external systems that will further extract value from the existing scope, and at the same time also further significantly enhance good business process.

The systems that are pre-identified to progress during the JISC pilot phase are:

1) Library Management System – We have committed to provide a link to the current Library Management System, which exists as an entirely stand-alone database requiring the re-entry of all student records as a manual process. The technique to manage this link will need to take into account that only minimal support from the vendor, whose facilities to approach interoperability is most closely aligned to a specific product suite only. In this instance, a method that perhaps bridges a rather crude data import and export facility to a controlled and verified link to our data vault may be the appropriate way forward.

2) Apple Macintosh network – The existing Apple network supports some three hundred plus workstations that have a loosely linked relationship with the "real" student record data. It is now an agreed goal that we will provide a bespoke link to provide a user data stream that is the same validated user database provided to users of PC workstations.

3) Google Apps – The current trend within educational institutions to make use of Cloud Computing facilities, such as those provided by Google, is something that needs to be embraced but in a way that clearly associates that remote data with the real individuals who own it. If we are to encourage our student learners to use this service then we need to be

able to validate their usage and content. It seems entirely possible that we can provide a management bridge between these remote Cloud based resources to link with our own definitive Student Record System.

These are the minimum goals of the next phase, but in reality we will also seek to bond and share data further between our existing interoperable services, and have a particular desire to link the finance system directly to the other key systems that support the business of the college. The successes demonstrated by the first phase were apparent to the management of the Finance department to enquire as to whether this system could also be linked in.

Summary & Reflection

This Pathfinder case study seeks to capture four years of development of interoperability and 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. 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.

The single area that comes so 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 other 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 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.

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 discipline to incorporate other business systems, demonstrating increasing return of investment.