

# The Identity Project

Common Challenges, Solutions, Best Practices and  
Future Developments for Identity Management in  
British Higher Education

**October 2007**

## EXECUTIVE SUMMARY

- Most institutions have developed single credentials environments whereby an individual is able to sign on and access a system with a single username and password.
- The majority of institutions report good awareness and compliance with the Data Protection Act and other relevant regulations.
- Institutions reported considerable attention to verifying an individual's identity prior to entering them into their system.
- There was a lack of common understanding or interpretation of the term 'identity management' across the HE and FE sector, as shown in the broad survey and the 10 in-depth case studies.
- British HE and FE institutions tend to operate independent, disparate systems of identity management. This may be due in part to the decentralisation and heterogeneity of different departments, research groups and other organisations within an institution.
- There are limited formal procedures and common standards for identity management across institutions.
- Issues such as deprovisioning of identity (e.g. such as an email account after a member leaves) and managing the quality of data across a decentralised identity management system remain key challenges.
- A number of institutions tend to use unique user credentials (i.e. a continuous form of identity for an individual that follows his or her changes in status within an institution, e.g. from student to staff member). This may be due to insufficient tools to identify prior identity of an individual.
- Future work on identity management could include the development of documented procedures and common standards, raising awareness of identity management throughout the institution and the introduction of regular audits.

# TABLE OF CONTENTS

<b>1. Introduction</b> .....	<b>5</b>
<b>2. Project Partners in the Institutional Audit Case Studies</b> .....	<b>7</b>
<b>3. General Characteristics of Partners Participating in the Institutional Audit Case Studies</b> .....	<b>8</b>
3.1 Origin of Organisational Structures.....	8
3.2 Groups' Autonomy .....	8
3.3 Implementation and Enforcement of IDM Policies .....	9
3.4 Characteristics Summary.....	9
<b>4. Common Challenges and Solutions</b> .....	<b>10</b>
4.1 Limited consensus on defining "Identity Management" .....	10
4.2 Heterogeneity – Independent, Disparate Systems.....	11
4.3 Limited Deprovisioning.....	12
4.4 Formal Procedures .....	13
4.5 Common Standards and Central IDM Administration .....	144
4.6 Identity Management Data Quality .....	15
4.7 Use of Non-unique User Credentials (per individual at the same time). 16	
4.8 Policy of Reuse of Identifiers .....	16
4.9 Adherence to the Code of Practice for Information Security Management (ISO 27001 Standard).....	17
4.10 Common Challenges and Solutions – Summary.....	17
<b>5. Best Practice</b> .....	<b>18</b>
5.1 Unique Identifiers .....	188
5.2 Single Credentials Environment and Security Trade-offs.....	18
5.3 Compliance with Data Protection Act and Other Relevant Regulations	18
5.4 Good Initial Identity Verification.....	19

5.5 Strict Physical Equipment Security .....	19
5.6 Use of ID Cards as Payment Cards .....	19
<b>6. Future Developments .....</b>	<b>20</b>

# 1. Introduction

This report concerns two requirements of the Identity Project: first, to uncover common challenges and solutions to issues of identity management (IDM) across the British academic community; second, to identify cases of best practice and areas for further development.

The Identity Project sought to identify how IDM is carried out in the British academic sector. The purpose was to assess the current state of practice and future needs of the academic community in this regard. A wide range of IDM issues were addressed, from those specific to an institution to those across the academic sector, including Grid use, Shibboleth installations and other inter-institutional collaborations. The timeframe for the Project, including data collection, analysis and the drafting of the various reports associated it took place between November 2006 and October 2007.

The Identity Project consisted of two main forms of data collection, from which a series of different reports have been produced: the first consisted of a broad survey sent out to all HE and FE institutions; the second involved 10 in-depth case studies of London-based HE institutions and partners in the Identity Project. The data from these two approaches form the basis of this report, along with other reports that have similarly been generated through the course of the Identity Project. These other reports include a quantitative analysis of the findings from the broad survey, qualitative studies of each of the 10 case studies, a study of membership across the 10 institutions, IDM and the NHS, the Grid and the tools used in IDM by the sector.

The Identity Project collected data on IDM in two main ways: through a broad survey and 10 in-depth case studies. The broad survey was managed by Cardiff University and consisted of a paper-based (rather than web-based) exercise and was sent out to 184 HE institutions, generating a response from 53, or 28.8% with a broad representation across the UK. A range of single-choice, multiple-choice, open-ended and closed questions were asked, covering the role of the IDM team at the institution, their policies, efforts to integrate data, use of technology, the NHS and Grid and other collaborations. The broad survey was publicised at various IT-related events and despite an 18 May deadline, responses were accepted until the end of the Project in October 2007.

The findings of this survey suggested that every institution shares a number of core challenges with regard to IDM procedures and policies, both technical and political. Solutions to these challenges range from simple technical fixes to necessary changes in procedure and policy that require buy-in from senior management.

The 10 in-depth case studies consisted of predominantly London-based institutions, under the management of the LSE Information Services team. Key researchers were appointed in each institution to be studied, which included the Cardiff University, the LSE, Birkbeck College, Goldsmiths College, Imperial College, Queen Mary College, Royal Holloway, SOAS, University College London and the External Programme at the University of London. In March and May 2007 meetings were held to determine the form of the methodology, establish what constituted IDM practice (or not) and to identify relevant informants between the key researchers and the LSE-based management team. Following these meetings the lessons from these meetings were used as a series of face-to-face interviews were conducted during

the summer months and the findings relating to IDM issues analysed. The analyses led to the drafting of individual reports on each institution in August-September 2007.

The work from the individual case studies augmented that of the broad survey by seeking information on what institutions deem to be their biggest challenges regarding IDM. The project team also sought to identify solutions to these common issues, either through technical solutions, or, where the problems are political or procedural, the project team communicated with stakeholders and the community at large to help reach a consensus as to the best possible solution(s) to these problems.

Despite two distinct approaches – the quantitative analysis generated by the broad survey and the qualitative from the in-depth case studies – both have fed into the various outputs envisaged by the Identity project. This has included cross-institutional studies on the role of membership, collaboration with the NHS, the Grid and various IDM tools used by the academic community, all of which are available elsewhere.

For the purposes of this report, the same set of findings from the two research methods were used by the management teams at LSE and Cardiff sought to highlight examples of good practice for IDM procedures, policies, systems and tools for academic institutions enabling them to operate effectively in the UK Access Management Federation; and to allow their users to make effective use of Virtual Organisations. It also sought to establish a direction for Future Developments by the JISC and institutions regarding IDM, detailing areas in which further investigation would be beneficial to both the JISC and the academic community.

The above was accomplished by establishing a community consensus of the best IDM practices. The community consulted here consisted of all UK academic institutions, the projects involved in the other JISC e-Infrastructure Security project strands, the international community, and any other relevant stakeholders. The consultation took place throughout the lifetime of the Identity Project.

This report aims to highlight the common challenges, solutions and types of best practice that have been found through the various research in the Identity Project. Consequently it does not make direct references to individual institutions. This is due in part to the range of methods and size of the studies used to carry out the research. Whereas the broad survey was quantitative in scope, that of the in-depth case studies was primarily qualitative. It is therefore debatable to what extent the detailed findings of the in-depth studies are directly comparable to the more less detailed, but larger findings of the broad survey.

## **2. Project Partners in the Institutional Audit Case Studies**

The in-depth case studies took place in 10 primarily London-based institutions between March and September 2007 under the management of the LSE's Information Services team. The institutions included Cardiff University, LSE, Birkbeck College, Queen Mary College, Goldsmiths College, University College London, Royal Holloway College, Imperial College, London, School of Oriental and African Studies and the External Programme at the University of London.

The research was carried out by involving staff at each partner institution. They are known throughout the project and in this report as Key Researchers (KRs). They were familiar with local organisational structures and requirements in their respective institutions. The overall findings of the in-depth case studies are given in TidpCsResearchReport.

The colleges participating in the in-depth case studies constitute a very broad selection. They differed in size, the variety of subjects taught and selection of research work carried. This was reflected by the services information provided at these institutions and diversity of IDM policies and practices deployed.

At one end of the spectrum there were very large colleges with a very broad range of subjects taught and areas of research like University College, London. On the other end there were smaller institutions like Birkbeck College. The special case in that respect was University of London, External Programme. It does not provide any courses directly and carries out very limited research. It rather co-ordinates external programmes that are provided by other colleges of the University of London.

Despite the differences in size and areas of teaching and research amongst colleges that were the subject of the in-depth case studies these institutions have a lot in common as far as problems and best practices are concerned. This can be attributed to the fact that all of them are teaching and research institutions, i.e. they have to accommodate practically the same business processes and their organisational structures were established in similar ways.

### **3. General Characteristics of Partners Participating in the Institutional Audit Case Studies**

#### **3.1 Origin of Organisational Structures**

Most (if not all) partners institutions have been developing as a result of various mergers from other independent institutions. For example, Queen Mary College is a result of earlier merger of Queen Mary College and Westfield College. Imperial College, London incorporated a few years ago Wye College and University College London incorporated the Physics Department from Birkbeck College. Although such mergers result in the unified administrative structures, information systems are not necessarily fully integrated. This can be due to costs of such integration, perceived as excessive, i.e. uneconomical. Sometimes the benefits of integration do not justify the costs. There are also organisational and practical considerations like preserving control over local systems that reflect administrative arrangements.

Such practice, over the years, results in a large number of independently and semi-independently administered information systems, each of which quite often runs its own IDM modules. This entails that different programs and practices are deployed to run various systems.

#### **3.2 Groups' Autonomy**

Academic groups (departments, research groups, etc) like to keep their autonomy. They quite often perceive any intrusion from the outside (like central computing services) as necessary overhead at best, or sometimes, as unwanted intrusion. It occurs that a research group is awarded a grant and they buy their own new system or systems and set them up with little (or sometimes without any) co-ordination from central computing services that are responsible for central IDM administration. This poses both technical and organisational challenges for the institutions. Generally it can be said that this problem is more prevalent at institutions with large and prominent science departments. It appears that colleges that do mainly non-science subjects are less exposed to such phenomenon.

Addressing the groups' autonomy is a challenge. But it has also been observed that gradually a lot of these "independent" groups started appreciating the benefits of centralised IDM administration and they, themselves, ask for support when they install new systems.

### **3.3 Implementation and Enforcement of IDM Policies**

Generally it has been observed that all institutions have some formal policies regarding IDM, especially with respect to identity security. But there is little practical translation of these policies into practical specification standards that could be implemented throughout institutions.

There are also limited audit procedures that are actually carried out. So a lot of problems are identified by chance or when, for example, a security breach is very severe. (There are notable exceptions to this observation: mission critical or sensitive systems, e.g. finance, HR, which are well maintained from security perspective.)

The issues of implementation and enforcement of IDM policies are closely related to the compliance of ISO 27001 standard and are addressed in Section 4.8, Adherence to ISO 27001 Standard. (The Identity Project makes a reference to this standard only with respect to Information Security.)

### **3.4 Characteristics Summary**

These three characteristics, listed in the Sections 3.1, 3.2 and 3.3 above, are major contributors to the actual IDM policies and practices that developed in the partners institutions. It should also be noted that they both give rise to common problems occurring at these institutions. They quite often form the background of the best practices that have been developed.

## 4. Common Challenges and Solutions

### 4.1 Limited Consensus on Defining “Identity Management”

The Identity project opted to use the term “Identity Management” (IDM) as described in Wikipedia. This deems IDM to be:

- “1. the identity is established:
  - 1. a name (or number) is connected to the subject or object;
  - 2. the identity is re-established: a new or additional name (or number) is connected to the subject or object;
- 2. the identity is described:
  - 1. one or more attributes which are applicable to this particular subject or object may be assigned to the identity;
  - 2. the identity is newly described: one or more attributes which are applicable to this particular subject or object may be changed;
- 3. the identity is destroyed. “

[[http://en.wikipedia.org/wiki/Identity\\_management](http://en.wikipedia.org/wiki/Identity_management) – accessed 23 October 2007]

The broad survey tried to verify whether the term “Identity Management” is often misunderstood. It observed that “the lack of common understanding of what are its main aspects can be a hindrance to institutions wishing to conduct IDM projects.”

It has been identified that some 70% of the respondents to the broad survey indicated that “IDM encompasses the provisioning and deprovisioning of access to an institution’s systems”. However, there was a scope that the use of the term “Identity Management” in general may be a source of some confusion and misunderstandings. In the background there is a wide and abstract meaning of this term. Hence for security staff who are checking personal identities of individuals, identity management is associated with physical access. On the other side, for system administrators, the term “Identity Management” may be synonymous with user account management or even as specific as user security.

The lack of commonality in understanding and usage of the term “identity management” may potentially lead to misunderstandings in the process of management and administration of IDM related projects. The lack of common standards and uniform documentation (to which this document makes a reference later) can also be partly attributed to the lack of uniform understanding of the term of “Identity Management”.

## 4.2 Heterogeneity – Independent, Disparate Systems

Each of the Project partner institutions consist of a number of faculties, departments, centres, research groups etc. Each of these units run their own academic research and teaching programmes. Quite often, for the purpose of the local use, systems are set up in order to support local unit's activities. As a KR stated: "Academic departments and research projects (especially well-funded ones) have historically been rather autonomous and are not always keen to participate in centralised management." This results in a number of systems, which are not supported by the central administration team responsible for IDM. Such an arrangement may lead (and sometimes it does) to multiple identities issued to the users that need to be managed by an institution.

A solution that has been identified in over half of the partner institutions is keeping the same credentials environment: i.e. individuals are given a single username and password. Some partners institutions actively encourage that. The remaining drawback is that it still requires to keep multiple records of the single identity in various systems. This entails duplication of data held. There is a risk that these duplicate data records will, in time, become inconsistent.

On the organisational side, some departments or research groups employ their own system administration staff. They co-ordinate local (departmental or group's) IDM administration with a central support IDM team. However, it also happened that there are local research groups that do not have a proper support team and the whole system administration (including IDM) is done in an ad-hoc manner. Such arrangements pose the biggest challenge.

To overcome that, the institutions encourage centralising IDM administration where possible.

The ultimate solution is implementation of a single sign-on environment. Central systems administration staff are responsible for the administration of the IDM aspect of all systems including local (departmental, research groups) systems. There is a growing awareness of the benefits of such an approach in most institutions.

It should be noted however that there are also situations where heterogeneity is beneficial for security reasons. Critical systems (e.g. in finance departments) and systems storing sensitive information (e.g. Registries) are kept outside of the central IDM administration for security reasons. Whilst it creates some inconvenience for the users (necessity of multiple sign-on's) and gives rise to some system administration overheads, including IDM, it provides a more secure corporate environment.

Generally, central systems administration teams that manage identities for an entire institution do not get directly involved in IDM on the local level system (departments or research groups). The practical solution that reconciles the heterogonous management environment (including IDM) with the need of central administration involves:

- good coordination between central system administrators and local systems administrators;

- introduction of single credentials environment, based on the central system, prospectively leading to the introduction of single sign-on (except for some systems that for security reasons should remain outside of such an environment).

### 4.3 Limited Deprovisioning

It was identified that the problem of non-consistent deprovisioning exists amongst the project partner institutions. Users, e.g. students, employees, are assigned credentials and given access rights to a range of resources at the institutions. However when a user moves through different positions or assignments in the institution, his access rights must be varied accordingly, and ultimately, when he leaves, his credentials should be removed.

It has been noted that there are some problems with managing users' rights and removing credentials. This closely relates to the management of different categories of users. With respect of categories:

- employees
- students

they are managed quite effectively, provided they remain within generally prescribed standards (being an employee or a student). However, problems start when either an employee or a student falls outside of these categories. For example, a student is given an extension to complete a project, or a research student becomes also a research assistant, or a member of staff is assigned duties that are beyond his standard scope of work, which require additional access to resources. Typically the provisioning process works reasonably well. It is usually an execution of requests for access or extension of rights, which if not done, are the subject of repeated requests or a complaint.

The deprovisioning process is more cumbersome. Usually a user does not notify IDM administrators that he does not need access to some of the resources or should be removed as a user. Therefore a number of users' assigned credentials and/or access rights stay on the system whilst they should have been revoked some time before.

There is a number of users at each institution that can be described as non-standard. Although the non-standard term can be interpreted very widely, any user who is not a student or an employee can be broadly considered as non-standard.

Most of the partners institutions are trying to standardise these non-standard users. Nevertheless it appears next to impossible as there is a wide variety of them. Similarly to the problems presented above, the process of deprovisioning of non-standard users is very challenging. Very often it requires the proactive co-operation of a non-standard user sponsor (for example a professor who is the sponsor of a visiting researcher at an institution). Unless a sponsor notifies the IDM administrator that non-standard user's access rights should be

changed or his credentials should be removed, such a user can stay registered and provisioned well beyond the prescribed period.

The other effect of deprovisioning problems is that some users move from various positions in an institution and they accumulate more and more access rights to resources, e.g. access rights to resources they do not need anymore are not revoked.

The general solution to deprovisioning problems is imposing time limits on credentials. Whilst this solution works reasonably effectively on access rights that give physical access (e.g. ID cards) it can cause problems when it is imposed on electronic resources. For example, if an employee, a member of senior research staff, is denied access to resources, or if his credentials are revoked, it can cause administrative complaints and be a cause of additional work. This can also be a source of embarrassment. However the time elapsing approach to credentials management is quite widely implemented with managing large groups like students.

Sometimes heads of departments or research groups notify IDM administrators when a member of staff or a non-standard user (e.g. a research fellow) leaves the post. This has not been observed as a standard practice, but a rather rare ad-hoc action.

Another solution is carrying out IDM audits. Audits allow the institution to determine users that still require credentials, access to a range of electronic resources and physical access. Carrying out audits requires the full co-operation of administrative and academic staff who are responsible for users. Generally, across the institutions researched audits are carried out infrequently, usually on an ad-hoc basis. There is also a lack of deprovisioning formal procedures and enforcement mechanisms. Deprovisioning is quite frequently governed by custom and practice, which are very often unclear or depending on subjective judgment of a person responsible.

Deprovisioning of non-standard users is arguably the most difficult problem that IDM administrators face. It encompasses many issues related to the autonomous character of departments and research groups at colleges and implementation of standard IDM policies.

Inadequate deprovisioning policies and procedures amounts to a breach of the ISO 27001 standard that requires reviews of all account privileges.

#### **4.4 Formal Procedures**

Every Partner institution operates formal policies regarding ICT management, including IDM administration. However, on many occasions these policies:

- do not cover all the IDM related areas
- are not translated into formal procedures or technical specifications

- are not enforced throughout the organisation.

In such an environment, the problems resulting from the lack of procedures are alleviated by informal contacts and undocumented knowledge on “how it works” by the staff. As one KR commented: “There is insufficient documentation for someone to know how to create credentials in any of the (...) systems without external input, but the procedures for doing so are known by more than one employee.” Another KR commented: “First problem is culture: (it is difficult) to impose official policies.”

The lack of properly implemented formal procedures sometimes gives rise to cases of IDM administration without clear overall control and without clearly defined lines of accountability. A KR remarked with respect to a partner institution: “There is no central place where every research group and every academic or administrative department or business unit is listed”. It was also remarked that “a lot of process are mysterious”.

Sometimes the lack of or inadequate formal procedure gives concerns to the level of security. “There are some policies on security but (they are) not implemented or dead” (i.e. completely inactive). A KR continued: “Security is quite often considered as optional. Solutions are imposed first – security is added as a ‘bolt-on’”. Sometimes it results in “woolly” (as another KR remarked) security culture.

It should be remembered that the extent of inadequate formal procedures varies across partner institutions or even across departments or research groups within a single institution.

As “generally there is a desire to have good security and IDM administration”, these challenges are addressed by “not formal, unwritten code of practice”. This ensures that certain sensitive or critical systems, like in Finance, Registries or HR are given special attention and are administered under the close eye of people directly responsible for these systems. Overall it leads to a reasonable level of control and security. The drawback is the lack of central IDM administration and “very little coherent integration”. To conclude, in many situations, “lack of documentation – get away due to (good) practice”.

The lack of or inadequate formal procedures amounts to non-compliance to the ISO 27001 standard.

#### **4.5 Common Standards and Central IDM Administration**

The lack of common standards and central IDM administration is related to the organisational structures and groups’ autonomy at partner institutions. For example, there are “no particular metadata standards used for person data”. The autonomous character of various departments, faculties and research groups leads to the variation of standards and decentralisation of IDM administration. The consequence of such a situation may lead to other problems. This can be:

- inadequate deprovisioning practices (including non removal physical access, a serious security issue)
- multiple identities (which in some partner institutions is very common)
- non-uniform access across departmental systems within a single institution
- non-unique or non-consistent ID (potentially leading to ID ambiguities).

The overall solution identified amongst partner institutions to the lack of common standards and central IDM administration is the custom, practice, cooperation and experience of the staff. Whilst it has to be acknowledged that this is not a desired method, it is a pragmatic approach. The growing awareness of the need of centralisation, or at least coordination, helps to minimise the effects of the lack of standardisation and central IDM administration. But quite often, the resulting practices are of informal character and their application depends on local knowledge and the good will of the staff.

The lack of common standards and lack of central IDM accountability amounts to non-compliance to the ISO 27001 standard.

#### **4.6. Identity Management Data Quality**

It has been observed that, on many occasions, IDM data is not accurate. The data is either incorrect or it is not fit for purpose. The former usually is related to the manual input of data. The solution to this problem is minimisation of points of manual data entry and use of automated data transfer and reconciliation.

The other problem relates to “repurposing of data”. As an example: a partner institution reported that one application took student module enrolment data from a different, student records system. Students’ records system was adequate for the Registry’s purposes, that module enrolments be updated in time for Registry’s business needs, such as production of the examination timetable in November. However, the process was not adequate for the other system’s needs which required the data to be correct on the first day of teaching.

One partner institution commented: “If a new piece of identity information is made available and another application uses that information, a complete understanding of that information is necessary. This includes such things as an understanding of how the information changes over the cycle of the academic year, how timely the information is updated, what every state of information means, and what permission a system has to pass on this information to a further system.” The comment went on further: “it takes at least one full academic year to understand a piece of identity information well enough to use it in a different system without encountering problems.”

## **4.7 Use of Non-unique User Credentials (per individual at the same time)**

In some institutions (around a half) an individual may be assigned more than one set of credentials, i.e. username and password, at the same time. For example, this means that if someone is registered as a student at a university and later, whilst still being a student, starts working at this university, then his user credentials given to him as an employee will be different than ones that were given to him as a student. Furthermore the individual records as a student of that individual may not be linked to his employment records or an account as an employee. Such policy, whilst quite straight forward to implement, carries an almost certainty of records related to the same individual being associated with different credentials, distributed in the institution's system and difficult to trace. Matching different records of the same individual is a very difficult, forensic exercise. It also carries a realistic risk that the records of different individuals may be merged.

These practical problems would arise when an individual makes a request under the Data Protection Act. There is a reasonable risk that if a complete set of this individual's credentials are identified, he will not be provided with a complete set of records regarding himself.

On the other side, if such an individual is associated also with credentials of some other individual, he would be possibly disclosed illegitimately confidential information about somebody else.

Both these scenarios are difficult to prevent under a Non-single User Credentials policy.

Sometimes a non-single credential environment is a result of inadequate implementation rather than a matter of the stated policy itself. An institution may have a single credentials policy, but it may not have sufficient tools to determine whether an individual has been assigned credentials before unless an individual discloses quite detailed information. A few institutions carry prior user discovery procedures. However these procedures do not appear fool-proof: as there is a risk that an individual may be assigned with somebody else, to be on a safe side, an individual may be assigned new credentials.

## **4.8 Policy of Reuse of Identifiers**

When an individual leaves an institution his (or her) credentials and identification data are retained for some time (e.g. two years) and then it is reused. In such circumstances, a returning individual is likely to be assigned new IDM credentials when he re-joins the institution. Furthermore, someone else could be assigned his credentials (e.g. e-mail address). Whilst, generally, for the purpose of an institutional internal use, such a policy is adequate, it carries certain risks if someone is assigned some else's e-mail address. A new user may become a recipient of the previous users e-mail correspondence.

#### **4.9. Adherence to the Code of Practice for Information Security Management (ISO 27001 Standard)**

At the outset of the Identity Project, the LSE and Cardiff management teams sought to discover the extent to which HE and FE institutions made use of international codes of practices relating to IDM, in particular the ISO 27001 Standard. However, neither the broad survey nor the in-depth case studies identified active adherence. This is not to state that the partner institutions do not follow some of the requirements stipulated by the standard relevant to IDM, but such adherence is the effect of internally developed policies and practices.

In particular, the standard stipulates that documentation reflects management commitment to IDM policies, gives details of relevant legislative and regulatory requirements and includes clear descriptions of what should be done in case of security violation. Such strict approach has not been identified amongst the partner institutions.

The lack of confidence in the IDM data records integrity also suggests that ISO 27001 standard is not strictly adhered to. There were also no formal and regular IDM-related risk assessment procedures or audits, as stipulated by the standard, identified. The reuse of credentials in some institutions also is in breach of the standard.

#### **4.10 Common Challenges and Solutions – Summary**

It has been noted that ALL challenges related to IDM administration occur in ALL partner institutions. The extent of these problems does vary from institution to institution. This does depend on both the complexity of the institution and the level of implementation of IDM systems, policies and procedures.

Generally stricter adherence to ISO 27001 would be beneficial in providing solutions to the existing problems. There would be however important considerations in relation to costs, administrative overheads and timescale.

## **5. Best Practices**

Whilst carrying the Institutional Audit Case Studies at partner institutions, we have identified a range of practices that deserve to be recommended. These practices were not necessarily present at all institutions. Sometimes they are also not implemented across a single institution where they were identified.

### **5.1. Unique Identifiers**

It is generally acknowledged that each individual should be associated with a single unique identifier for life. Some institutions made efforts in order to implement and use such approach.

### **5.2 Single Credentials Environment and Security Trade-offs**

Most institutions report a wide implementation of single credentials environment, i.e. single username/password set up per user. However a user may be required to enter his credentials on numerous occasions whilst using a computer system. Furthermore the single sign on environment is not implemented.

It should be noted that with sensitive or mission critical systems, for example in Finance, Registry or HR, institutions tend not to use single credentials set up. (For example, for a particular user, there is different username/password pair for ordinary administrative file server and financial reporting system.) Whilst such an arrangement is seemingly rather less comfortable to a user (than single credentials environment), it enhances security. It was pointed out throughout the audit process that such exceptions have really been justifiable, well thought out exceptions. It was observed that this trade-off was balanced as too many username/passwords usually leads a quite lax confidentiality: e.g. staff tend to write them on post it notes.

By and large, it appears that partner institutions seemed to have managed to strike the right balance between simplicity and security.

### **5.3 Compliance with Data Protection Act and Other Relevant Regulations**

All partner institutions put a lot of attention and effort to comply with all requirements of Data Protection Act and other legal regulations. It was not the purpose of this Institutional Audit Study to look closely into such compliance. However, the general approach and attitude do not bring to light any immediate concerns. It was noted that institutions make pragmatic decisions with respect to security and that the “culture is getting better”.

## **5.4. Good Initial Identity Verification**

All Partner institutions carry very stringent initial identity checks on individuals that are to be issued with standard credentials (new students, new employees). It is done usually by presenting by an individual a passport or some other strictly defined acceptable set of the identification documents. This initial identification procedures are well defined and appear to be strictly adhered to.

## **5.5 Strict Physical Equipment Security**

Most Partner institutions reported a very strict physical security of critical information systems equipment, especially network equipment.

## **5.6 Use of ID Cards as Payment Cards**

One Partner institution reported an implementation of the application that enables the use of an ID card as a payment card for college printing and photocopying services. Such an ID card has a monetary value. As a result this limits ID card usage abuse especially amongst students. For example, generally student lend ID cards to each other (and even possibly others outside of the institution). Such behaviour has obvious implications upon the general security but there is also a risk of wider implications. For example an access to some library or electronic services may be based on ID card. Lending cards can have legal implication upon licensing issues.

The use of ID cards for other purposes (e.g. as payment cards) is an innovative best practice that is recommended.

## 6. Future Developments

Universities and colleges are very large and complex organisations. Generally the IDM fits the purpose it serves and adheres to statutory requirements. In order for the organisations to develop further in the area of IDM the following issues should be addressed:

- improved documentation and standards – each organisation should develop, implement and maintain their own IDM standards, policies and procedures; these standards and documentation should encompass both centrally managed IDM systems as well peripheral and satellite systems that exist in departments and are maintain semi-independently from central systems; it is acknowledged that a complete centralisation and integration is not feasible, however coordination can be improved;
- improved awareness – to achieve improved management and coordination of administrators there should be more IDM training available; the improved awareness together with consistent standard and documentation should result in higher IDM level of service across universities and colleges.
- introduction of regular audits – to ensure an appropriate quality of IDM documentation and standards, and also level of IDM awareness amongst the staff, each institution should set up a regular audit process; the precise form of this process should be up to each individual institution; for example it may be carried out by a separate unit formed or group of professionals seconded from other units; it should be noted that an IDM audit unit has to have sufficient standing within the institution so its recommendations are implemented by all responsible of IDM.

The introduction of IDM audit unit addresses some issues uncovered in the course of this Institutional Audit Case Study: groups' autonomy, heterogeneity and lack of central IDM administration. Whilst it seems rather impractical or even impossible to completely integrate and unify IDM administration, IDM audit unit should be instrumental in creating semi-integrated IDM environment.

The audit units should be guided by the ISO 27001 standard and also take an overall responsibility of an institution's adherence to them.

Better documentation and standards combined with high level training and resulting awareness, monitored and sustained by regular audits, should create good foundation for federated access implementation projects.