Identity Management

Project Scope
### Document Control

<table>
<thead>
<tr>
<th>Version #</th>
<th>Change Description</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Initial draft to Steering Committee members</td>
<td>16/7/07</td>
<td>Jane Florey</td>
</tr>
<tr>
<td>0.2</td>
<td>Draft incorporating suggested changes</td>
<td>24/7/07</td>
<td>Jane Florey</td>
</tr>
<tr>
<td>0.3</td>
<td>Draft incorporating further changes</td>
<td>30/7/07</td>
<td>Jane Florey</td>
</tr>
<tr>
<td>1.0</td>
<td>Sponsor approval</td>
<td>31/7/07</td>
<td>Jane Florey</td>
</tr>
</tbody>
</table>
Identity Management Project Scope
Table of Contents

1 PROJECT PURPOSE STATEMENT: .................................................................4
2 BACKGROUND: ...............................................................................................5
3 OBJECTIVES: ......................................................................................................5
4 KEY STAKEHOLDERS AND OTHER PLAYERS: ..............................................7
  4.1 ROLE OF THE PROJECT MANAGER .......................................................... 8
  4.2 ROLE OF THE PROJECT STEERING COMMITTEE ....................................... 8
5 ORGANISATIONAL REQUIREMENTS .............................................................9
6 APPROACH .........................................................................................................10
7 TIMEFRAME & MILESTONES .........................................................................11
8 INCLUSIONS & DELIVERABLES .....................................................................12
9 EXCLUSIONS .......................................................................................................12
10 ASSUMPTIONS ..................................................................................................13
11 CONSTRAINTS ..................................................................................................13
12 RELATED PROJECTS ......................................................................................13
13 RISKS ................................................................................................................15
14 NEXT STEPS .....................................................................................................16
15 SIGN OFFS .........................................................................................................16
Identity Management Project Scope

1 Project Purpose Statement

The Identity Management (IdM) project has been established to review the identity and access management processes across UWS and provide unified, consistent and standard business processes and technology to support an individual’s relationship with UWS.

Information technology is embedded in almost every aspect of the activities undertaken to achieve the University’s mission. Effective use of IT is dependent, among other factors, on the provision of ‘the right access for the right people at the right time’. The ‘right access’ refers to authorised, streamlined access to IT services. The ‘right people’ refers to members of the UWS community (ie staff and students of all types), visitors and others (eg contractors, vendors, agents or individuals in the wider community) who have an authorised relationship with UWS. The ‘right time’ refers to timely provision of access from the start of a person’s relationship with UWS until termination at the appropriate time.

Coupled with the effective use of IT by authorised entities is the consideration of appropriate security of the university’s IT services and data to prevent unauthorised access and this needs to be balanced against individual privacy considerations. Key to a successful IdM scenario is appropriate identity and access policy, management and administration.

The mechanisms that serve identity and access management of IT services can also be leveraged to manage more effectively access to other university services and facilities, eg library services, buildings.

With IT infrastructure and business changes around the unified UWS now complete, the foundation is in place for the next step in identity management at UWS. The need for more streamlined processes and the support of strategic objectives form the main drive for taking this next step, aided by recent technological advances in the identity management space.

As regards the University’s strategic objectives, IT is a key enabler. The IdM project will enable many of the strategic imperatives:

- Engaging in world-class research and securing future research funding will be strongly linked to our ability to participate in a federated model for collaborative research;
- Improved accessibility to resources will improve the students’ learning experience at UWS;
- Streamlined access to services not only within but also from outside UWS will enhance the sense of community, benefit community relations and contribute to making UWS an institution of choice for students and staff in an increasingly competitive higher education landscape;
- Reducing costs of licensing and administration will contribute to the financial and sustainability agenda.

The Business Case for this project was originally presented in a UWS Systems Budget proposal dated 31 May 2006 and has been re-presented in the document IT System Proposal – Identity Management v1.0 dated 12 June 2007.
2 Background

In the years 2001 to 2005, the strategic direction for IT at UWS was focused on establishing an Enterprise Architecture for the unified UWS. This Enterprise Architecture provided the foundation for the application of emerging technologies and service improvement programmes to support and enable the university’s business objectives. Identity management became an area of focus at this time.

Some initial research work carried out in 2006 identified the need for refined business processes and a technology solution to deliver widespread benefits in the area of identity and access management. It was intended that this would take the form of a technical deployment in parallel with requirements definition for business process change and full technology implementation.

This project builds on the initial research but allows for a policy definition and detailed requirements analysis phase ahead of best-fit technology implementation and process change. Knowledge of and any associated documentation for the relevant policy, processes, architecture and system interfaces that make up the current IdM mechanisms are in pockets spread throughout various parts of ITD and the wider UWS. Furthermore, the vision of the required UWS IdM system model is not fully defined. The detailed requirements analysis is intended to address these encumbrances, as well as to deliver a defined technology and process change roadmap for the implementation phase.

Based on the 2007 system budget approval, the project was initiated with the recruitment of a Project Manager in May07 and the formation of a Steering Committee in Jun07. A 2008 systems budget proposal has been submitted to reflect the revised approach.

More background information on the current situation in the area of identity management is given in the next section.

3 Objectives

The high level project objectives described below fall in the following main areas of focus:

- User/account provisioning and de-provisioning
- Access control/management
- Wider application of Single Sign-On
- Password/authentication management
- Alignment with federated model as enabler for research collaboration.

A standard username and password credential set has been in use at UWS for a number of years in the form of MyUWSAccount. ITD has gradually increased the range of services that use MyUWSAccount as the authentication mechanism for permitting a user access. Where possible, and usually as part of the natural upgrade cycle, corporate applications have been migrated to the use of this same sign-on mechanism in place of local proprietary methods, each with their own maintenance overheads.

With the implementation of MyUWS Student Portal, ITD have furthered the common sign-on scenario by creating mechanisms for credentials to be safely passed from one application to another. This pass-through authentication is in use for
MyStudentRecords (MySR), Platform Web tutorial registration and results processing and e-Notice. Students who access these services from within the portal have only to present their credentials once.

This project seeks to extend this limited Single Sign-On arrangement to the wider UWS community, such that members of the UWS community log on to a portal and thereby gain access to the services they require without having to re-present their credentials.

With extended Single Sign-On comes increased risk to data should the ‘master key’ be compromised. However, this project will allow for consideration of raising levels of assurance in applications that currently may not have strong authentication built in by strengthening the authentication mechanisms for Single Sign-on through the use of more than one factor of authentication. Hence, this project will also implement an appropriate strategy for password/authentication management in terms of type, format, refresh etc.

Currently, inconsistencies exist in user/account provisioning and de-provisioning. For instance, variable delays are experienced before a new staff member is provisioned with a MyUWSAccount and access to basic networked services (eg email, My Documents, file shares, printing, internet). Also, much of this process is manually driven for staff through the use of forms. There are also inconsistencies in the type of MyUWSAccount provisioned. This project aims to streamline this process and introduce automation, ultimately being managed through a self-service application for the majority of cases.

Many members of the UWS community currently have multiple IDs because, for example, they are a student as well as a paid staff member. This situation creates inefficiencies in system administration/maintenance and is not an acceptable arrangement for the user community in many cases. This project will endeavour to resolve this situation to one of seamless management of multiple roles. This role-based access management model will also enable necessary variations in the de-provisioning of access to services (ie immediate cessation of access to Oracle Financials, but deferred cessation of access to email, for example).

The opportunity exists to address the scenario around access to services through the local wireless network when staff or students from another institution visit UWS or UWS staff or students visit another institution. Currently this can be a protracted process of approvals and administration on a case by case basis. This project will consider the streamlining of this process through ‘eduroam’, a gradually expanding confederation for educational roaming, enabling network access using home institution credentials for authentication to the local wireless network when visiting another member institution.

Currently, authentication to locally maintained directories for some applications exists and gives rise to duplication and inefficiencies. Through the employment of a role-based model for access to services and the application of more widespread authentication against an enterprise directory service, this project aims to benefit not only the user community in terms of a more seamless IT environment, but also to bring about efficiencies in the system administration area through the elimination or reduction of local authentication lists.

There is currently no single authoritative repository of information on individuals in the UWS community, eg for staff, the authoritative source for Name and Staff ID is not the same as that for location and telephone number. This leads to
inconsistencies and/or inefficiencies associated with applications that use these attributes. Whilst this is clearly related to identity management, an assessment will be needed to determine whether a single authoritative, accurate repository for UWS community member information is an objective of this project.

The access control component of identity management is not limited to IT services. The ID card system at UWS relies on the current IdM mechanisms for data to produce student-type and staff-type ID cards. The ID card system is currently operated by Student Centres. A separate system is used by Capital Works & Facilities to encode the cards with building access data and to encode separate cards for other individuals, such as building contractors. This project will seek to review the business processes in this area and, if appropriate, integrate this aspect of access management into the IdM system model.

On a strategic level, this project will provide the opportunity to adopt the necessary standards for future participation in a federated model of Service Providers and Identity Providers and thereby enable future research collaboration. Securing research funding in the future is likely to have a strong reliance on the ability to participate seamlessly in authorised sharing of data on research activities with other universities and possibly industry partners. This e-Research related objective has its roots in the Accessibility Framework, a partner framework to the Research Quality Framework (RQF) and part of the Backing Australia’s Ability government initiative. Further information can be found at: http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/accessibility_framework/

Other strategic objectives of UWS in an increasingly competitive landscape relate to attracting and retaining students and staff and building community relations. Initiatives that are likely to contribute to these objectives are e-Admissions and e-Recruitment systems for potential students and staff respectively and the Future Students project. The IdM project recognises these initiatives and will address the possible need to bring forward the time at which an individual’s identity is established to an earlier stage of a person’s relationship with UWS.

### 4 Key Stakeholders and Other Players

Key stakeholders in the project have been identified as follows. These areas will have representation as shown on the project Steering Committee.

- **IT Director (Sponsor and Chair)** – Mick Houlahan
- Office of Human Resources – Andrew Robb
- Office of the Academic Registrar – Stephen Pritchard
- Library – Lisa Tyson
- Office of Research Services – Debra Bailey
- Capital Works and Facilities – Peter Blunden
- Finance – Peter Noble
- Audit and Risk – Bob Johnson
- IT Strategic Planning Project – Kym Morris
- IT Security – Darren Geddes
- ITD Business Information Systems – Chris Alton

Other participants in Steering Committee:
Other stakeholders and interested parties in UWS will be invited to participate as appropriate during the project. These include (but are not limited to): Alumni, Marketing (Future Students Project), RAMS, University Engagement, Media and Communication.

Other players are likely to include technical and process specialists drawn from ITD and the wider UWS, who will be called upon for the Project Team and any focus groups, working parties or workshops convened.

In addition, it is likely that external consultants will be engaged in this project at various stages.

4.1 Role of the Project Manager

Specific responsibilities of the Project Manager include:

- Providing overall day-to-day management of the project;
- Providing leadership and management of the project team and managing financial, staff and technical resources effectively, to ensure the objectives and timelines defined by the Steering Committee are achieved;
- Developing the project approach and preparing and maintaining the project plans, schedule, resourcing and budget;
- Controlling the project through the preparation and maintenance of the required procedures and registers;
- Preparing and presenting regular status reports to the Project Sponsor and internal governance committees;
- Specifying and monitoring critical path dates and dependencies for the project so that specified completion dates are achieved;
- Leading and managing the identification of risks, and risk factors, affecting critical path deadlines and reporting to the project Steering Committee so risk factors are addressed pre-emptively;
- Identifying project deviations and implementing corrective action in a timely manner;
- Establishing and maintaining communication with all project stakeholders;
- Leading and managing activities to ensure that all relevant documentation is complete;
- Meeting records management, quality assurance and other policy obligations associated with the project;
- Where necessary, identifying suitable external resources to undertake certain tasks and acting as their contact point within UWS on this project;
- Acting as a liaison point for all activities related to the project.

4.2 Role of the Project Steering Committee

The Steering Committee will meet at designated points through the project duration. Specific responsibilities of the Steering Committee include:

- Providing advice and direction to ensure the successful completion of the project;
• Supporting the Project Manager in the accomplishment of project goals;
• Discussing, identifying and reviewing requirements/issues;
• Providing the necessary support to the Sponsor for sign-off on milestones and deliverables;
• Ensuring the commitment of required resources to the project;
• Coordinating, planning and implementing required actions to ensure project outcomes are effected;
• Monitoring the progress of the project and its impact on the University;
• Assisting with the resolution of issues that are outside the authority of the Project Manager.

5 Organisational Requirements

During the implementation of this project, IT services at UWS must continue to function in an efficient and effective manner. By the nature of this project, there will be changes to business processes and the introduction of new technology. However, the requirement will be to minimise and mitigate against disruption to staff, students and business operations.

Critical success factors to achieve these requirements are:

The project needs strong support from the heads of stakeholder areas and the University Executive and be recognised as of benefit to the university’s operational effectiveness and strategic imperatives;

The project requires a robust and effective governance structure that:
• ensures a whole-of-UWS approach,
• provides the necessary direction, and
• enables timely decisions to be made on policies and issues outside the authority of the Project Manager;

There needs to be an explicit and effective communication strategy that allows for:
• open communication between the Steering Committee, the Sponsor and the Project Manager, so that issues are visible, processes are transparent and decisions are accountable, and
• appropriate communication and consultation with end-users through stakeholder areas to ensure a common understanding of issues and decisions UWS-wide;

There needs to be a clear definition of relevant policy and guiding principles to provide the direction and boundaries for the development of the IdM model implementation roadmap;

Project plans need to have clear milestones and timelines, clearly assigned responsibilities and need to convey to stakeholders and participants the importance of timely completion of tasks and the implications of delays to project progress;

There needs to be due consideration and consultation of impact on staff, students and business operations through the stakeholder community and project governance;

The Project Manager needs to be afforded timely access to the required technical and process expertise and these resources need to be identified with adequate lead time;
Administrative support to the Project Manager will be required throughout the duration of the project.

6 Approach

It is intended to break the project down into two phases:

Phase 1:

Research and high-level requirements gathering leading to Scope;
Detailed project planning and risk assessment;
Identification and evaluation of potential ‘quick win’ implementations;
Establishment of guiding principles (to provide a high-level focus summary and framework for the following);
Detailed requirements analysis:
  Where we are now – current processes and technology/architecture;
  Where we want to be – UWS IdM model definition;
  Gap analysis – the difference between the target IdM model and the current scenario;
  Roadmap – what needs to be done to address the gaps, how and when this should be done and the estimated resources required;
Implementation of appropriate ‘quick win’ components (commenced in parallel with detailed requirements analysis if possible).

Phase 2:

Sub-projects and tasks to implement business process changes and technology components in accordance with implementation roadmap leading to the target UWS IdM model.

It is intended to conduct the detailed requirements analysis by engaging professional services. This approach will allow UWS to leverage the experience from other similar institutions. It will also allow in-house resources to remain focused on operational duties or other programmes of work to which they are already committed.

The implementation phase is also likely to involve engagement of consultancy, particularly with the technical deployment.

Working Groups will be convened at the planning stage of Phase 1 to progress various elements such as engagement of professional services for requirements analysis, risk assessment, identification of potential ‘quick wins’. It is intended to establish a core Project Team to oversee the implementation phase of the project. Working parties will also be established with responsibility to conduct specific elements of the implementation roadmap and any ‘quick win’ implementations.

Control of the project during both phases will include monitoring of progress against the schedule and maintenance of Issue and Change Control Registers according to associated procedures.

Upon completion of the implementation phase, a post implementation review (PIR) will be conducted prior to formal project closure. This is considered particularly
important for this project, as experience indicates that successful outcomes in the identity management area are achieved through iterative steps. In the interests of meeting project objectives, it will be necessary to adhere strictly to the project scope. However, over a project of this length, the landscape can change and further opportunities are likely to become apparent. Hence, not only will it be useful in the PIR to document the successes and lessons learnt from this project, it will be important to set a fresh baseline in preparation for any future work in the identity management 'journey'.

7 Timeframe & Milestones

The overall duration of the project is estimated to be two years, with a timeline and milestones as follows:

Phase 1: Requirements analysis and solution design

Initiating – May-Jun07 – identify and secure dedicated project resources, establish project governance, conduct research and high level requirements gathering and engage stakeholders, leading to approved Scope.

Planning – Jul-Aug07 – guiding principles definition and detailed planning, leading to Project Plan with Work Breakdown Structure (WBS) and schedule (Gantt chart), Communications Plan, Risk Management Plan, Roles & Accountabilities Plan, establish Working Groups, identify/evaluate ‘quick wins’.

Executing – Aug-Dec07 – engage professional services for detailed requirements analysis leading to implementation roadmap (Aug-Oct07); develop programme of work; undertake ‘quick win’ implementations (Nov07-Feb08 or earlier if they can be commenced in parallel with requirements analysis).

Phase 2: Implementation of process and technology changes in accordance with roadmap.

Planning – Dec07-Feb08 – expand Project Plan, WBS and schedule with details available from implementation roadmap and programme of work; revise other plans accordingly.

Executing (Stage 1) – Mar-Dec08 – implement elements of the programme of work scheduled for 2008 managed through working parties.

Executing (Stage 2) – 2009 – implement remaining elements of the programme of work which were not appropriate for inclusion in Stage 1.

Closing – 2009 - Post Implementation Review.

Milestones will be established in the Project Plan and progress towards those milestones monitored against the schedule. The quality of each milestone will be controlled by establishing criteria for success and evaluating each milestone against the criteria through timely project team and Steering Committee meetings.
8 Inclusions & Deliverables

This project embraces the business processes and technology associated with the following functions that support an individual’s or entity’s relationship with UWS:

- Identification – pre-assigning an identifier to an entity;
- Authentication – validating that an entity producing an identifier is the one to which the identifier was originally assigned;
- Authorisation – ensuring that the entity is afforded access only to the services and data required to support the allowed tasks;
- Accountability – ensuring that only the authorised entity can exercise its individual authority.

Deliverables throughout the project include:

- A documented review of the processes and technology across UWS that form part of the current system of identity and access management;
- Establishment or confirmation of relevant policy and guiding principles to provide a framework and direction for the target IdM model and the detailed requirements analysis;
- Definition of an IdM model that will provide unified, consistent and standard business processes and technology to support an individual’s relationship with UWS;
- Development of a roadmap for implementation of the target IdM model, documenting the gap analysis, the steps required to address the gaps and the estimated resources required;
- Implemented IdM processes and deployed technology according to the target model and roadmap;
- Relevant project documentation, including plans, schedules, procedures, registers, progress reports and a post implementation review report.

9 Exclusions

At this stage, it is assumed that this project will address role-based access management to a service, but not the access afforded within an application. For instance, an individual’s access to Callista will be managed by the IdM system, whereas an individual’s access to specific functions or data within the student records system will be controlled within the Callista application itself.

The management of operational issues arising with the current IdM system and any resulting changes to address those issues in the short term are outside the scope of this project (though such issues and changes must be brought to the attention of the Project Manager for assessment of the implications to the project). If, however, it is deemed that a workaround would temporarily address the issue, pending a longer term solution, the workaround would be outside the scope, but the longer term solution could fall within the scope, subject to an approved change request if necessary.

Any discussions or work undertaken regarding the use of real or fake personal information in test data is outside the scope of this project.
10 Assumptions

This scope is based on the assumption that funding will be available in 2008 for Phase 2.

The scope is based on high level research and initial discussions with stakeholder areas. Subsequent project stages may elicit new information that may give rise to a proposed change to the scope. In such cases, it is assumed that proposed changes will follow the change management procedure.

Further assessment of the projects listed in Section 12 below is likely to elicit further information which will clarify the scope of this project.

11 Constraints

Factors identified to date that may inhibit or restrict project delivery include the following:

Project progress will be constrained by the availability of resources designated wholly or in part to project tasks. Any discontinuity in this regard will impact project delivery, as it is anticipated that there will be limited ability to compensate for any resource unavailability.

Existing components of the current IdM architecture may restrict the project delivery in some way, particularly in terms of the starting point. These include:

- The MyUWSAccount identifier and the associated supporting management tools, which are well-established for staff, students and associates and are embedded into a number of existing processes;

- Active Directory, which is the established enterprise directory service and is most likely to remain so at least for file and print services.

12 Related Projects

Other projects that are likely to influence this project are as follows:

Internal

IT Strategic Planning Project – running concurrently until Dec07. Identity Management likely to become part of the program of work developed within the Strategic Plan.

Active Directory Health-check exercise - any project to carry out recommendations from this exercise (eg deactivating/deleting accounts, implementation of groups) may have an influence on this project.

ID card system replacement – target implementation at existing locations by November 2007. Any extension to the use of this system is outside the scope of the system replacement project, but instead falls within the scope of this IdM project.
e-Admissions system – an Admissions Management System (AMS) is currently in operation in UWS International for international students (system hosted externally). OAR is seeking to pilot an e-Admissions system for some students in 2008. This is likely to establish a potential student’s identity earlier in the process. It will also require the identification of ‘agents’ authorised to act on behalf of potential students.

e-Recruitment system – in line with the Our People 2015 project recommendations, the Office of Human Resources is seeking to implement an e-Recruitment system to automate the end-to-end recruitment process. This is likely to establish a potential staff member’s identity at the application stage.

Staff Profiles project – short-term exercise to deliver academic staff biographies via the Staff Directory over current infrastructure as an interim arrangement, pending more suitable accommodation of the requirements via the IdM project (specific details to be forwarded on completion of the Staff Profiles exercise).

Future Students project – a marketing initiative which is likely to give rise to another group of ‘new users’, though the current IdM arrangements have been used to provision access to groups of high school students. A post-implementation review of this exercise will be used to inform the project further in this area.

A UWS Business System Interfaces investigation is currently in progress in ITD that seeks to
• identify all of the data interchanges (interfaces) between major UWS systems
• identify and comment on the adequacy of existing documentation
• identify inter-dependencies between interfaces
• identify what integrity checks are in place, and
• describe any other special requirements that may apply to interfaces.
It is felt that the outcome of this study will be a useful source of information for the requirements analysis stage of this project.

ARROW institutional repository – being implemented by the Library and initially being populated to meet the requirements of the RQF, the ARROW repository will in the longer-term house research outputs of the University. Known requirements at this stage are secured access to materials by DEST evaluation panels, and the ARROW consortium has an authentication mechanism in prototype with DEST at present. Longer term however it may be necessary to implement alternate/additional authentication based on a variety of protocols, dependant upon roles of users. This will need to be reviewed post-RQF and may form part of the implementation phase of the IdM project.

External

Two projects that are likely to influence the IdM journey at UWS are as follows. Both are sponsored and funded by the Commonwealth Government as part of its Backing Australia’s Ability program, with the objective of providing researchers with access to an environment necessary to support world-class research.

Meta Access Management System (MAMS) project – a project to develop a prototype federated Identity and Access Management infrastructure for Australia’s Higher Education (HE) sector. Led by Macquarie University’s E-Learning Centre (MELCOE), this project aims to provide a ‘middleware’ component to connect people to a range of resources in distributed environments and thereby to increase the efficiency and effectiveness of Australia’s HE research infrastructure. These
resources include major research facilities, information and communications technology infrastructure, data repositories and other resources that support e-research, scholarly communication and collaboration and e-learning. This project may lead to the set of standards, schemas and technologies, to which a HE institution will need to align in order to participate in collaborative research using this federated model.

Further information is available at: http://www.federation.org.au/FedManager/jsp/index.jsp

The Australian Access Federation (AAF) project - this will build on an e-Security Framework project (based at the University of Queensland) and the MAMS project to develop and deploy an infrastructure to facilitate trusted electronic communications and collaboration within and between higher education and research institutions both locally and internationally as well as with other organisations.

Further information is available at: http://www.aaf.edu.au/

It is worth noting also the recent release by QUT of its Enterprise Sign On Engine (esoe), an open source middleware component that can provide a simple way for enterprises to join the Australian federation developed by the MAMS project. An evaluation would be required in comparison with other open source and commercial offerings as to its suitability to UWS and this evaluation falls within this project’s scope.

Further information is available at: http://esoeproject.org/

Another middleware initiative that is likely to influence the IdM project is ‘eduroam’ (educational roaming). This is an infrastructure based on a standard security technology which allows for inter-institutional roaming. It is currently active within an Asia-Pacific confederation and a European confederation. Being part of eduroam allows users visiting another institution connected to eduroam to log on (authenticate) to the wireless network using the same credentials that he/she uses at the home institution. Depending on local policies at the visited institutions, eduroam participants may also have additional resources at their disposal.

Further information is available at: http://www.eduroam.org/

13 Risks

A project risk assessment will be one of the first tasks to be carried out under the Project Plan and identified risks will be documented and controlled via a Risk Plan and Register. Risks associated with the identity management processes and technology will be addressed within the requirements analysis study. At this stage, the following risk areas related to the project have been identified:

Technical – relating to current infrastructure components and/or deployment of new IdM system components.

Scope – risk is that Scope creeps, impacting on timeline, resources and cost. Need to mitigate by strict change management procedures.

Skills and knowledge – risks around unavailability of staff with knowledge and skills required for particular parts of project.

On-going support – any hardware set up and software installations done by contractors carries a risk to on-going support and will be addressed through a programme of skills transfer to UWS staff.
Commercial - there are risks associated with the engagement of external consultancy because identity management is a complicated engagement. However, there are extensive risks in attempting an IdM project without the skills and experience of implementing IdM in a number of large complex organisations and with a sound technical knowledge of the chosen product framework, to ensure that our identity roadmap is realistic and achievable. Engaging external professional services aims to leverage these skills and experience, with associated risks controlled by careful requirements specification, tendering and selection of service provider.

A specific example already identified for closer assessment is Constellar Hub, a component of the current IdM architecture that performs the function of data integration engine. Possible risks are in terms of:

- diminishing commercial support for this product
- availability of staff for part of project timeline (mitigation action in hand)
- current function it performs is complex and bespoke and not easily replaceable with an interim solution before IdM system solution is implemented
- host hardware lease expiry (replace -> migration risk, extend -> hardware risk).

14 Next Steps

On approval of the scope, the following tasks will be undertaken:

Form Working Group(s) to assist with progressing Phase 1 elements;
Develop and agree a set of guiding principles (annexed to this document) to provide a high level summary framework for the detailed requirements analysis and a source of focus for the project;
Hold Project Kick-off meeting(s) as appropriate;
Develop Project Plan, Work Breakdown Structure, Schedule, Communications Plan, Risk Plan, Roles and Accountabilities Plan;
Establish Issues, Change Control and Risk Registers;
Conduct project risk assessment;
Conduct market research for and then engage professional services to conduct detailed requirements analysis;
Refine Project Plan and associated project management plans according to roadmap in preparation for Phase 2.

15 Sign Offs

| Project Manager | / | / |
| Project Sponsor | / | / |