# OE RESOURCE REQUEST APPLICATION

University of California, Berkeley

## I. SPONSORSHIP

A. Initiative

| | | | |
|---|---|---|---|
| Initiative | IT Infrastructure | | |
| Initiative Manager | Michael Mundrane | | |
| Phone | 2-6365 | E-Mail | mundrane@berkeley.edu |

A. Sponsorship

| | | | |
|---|---|---|---|
| Sponsor Name | Shel Waggener | | |
| Sponsor Signature | | Date | |
| | | | |
| Sponsor Name | | | |
| Sponsor Signature | | Date | |
| | | | |
| OE Program Office Signature | | Date | |
| | | | |

B. Give the title of the resource

| |
|---|
| Central Access Management System |

## II. PROBLEM STATEMENT/CASE FOR CHANGE

A. Identify and describe what needs the proposed solution is seeking to address.

1. Identity and Access Management (IAM) systems provide the foundation for creating and updating users' digital identities and managing access to electronic resources. As such, identity and access management plays a key role in "on-boarding" new students and staff, securing electronic resources so that only authorized users can access them, providing access to guests of the university, and generating audit reports to ensure compliance with policy and regulation. The lifecycle of every user involves multiple business processes owned and managed by multiple departments to ensure that:

- A CalNet or guest account is created
- Access requests for business systems are requested and properly reviewed
- Appropriate roles and access rights are assigned to individuals and groups
- Access is modified when a users' role has changed
- Access is removed when a user leaves the university

In an ideal world, these processes would be largely automated, efficient, accurate and userfriendly.
In reality, both the business processes and technology systems involved in digital account lifecycle management at UC Berkeley are inefficient, out-of-date, cumbersome to use, and not well-integrated.

2. Many campus departments maintain stand-alone user account systems specifically to provide access to university guests. Many of these departments would like to retire local account management solutions but cannot do so until a campus-wide approach to managing guest access exists. Departments can currently enter some types of non-standard university members into the HR system as "affiliates", but this is a cumbersome process and the overhead is too costly for many guests, like short-term conference guests or visitor who need wireless access.

With the support of the Identity and Access Management Steering Committee, the CalNet team formed a Guest Account Task Force in November 2008. Key stakeholders on this task force and the types of guest accounts they currently manage are listed in the table below (this list does not represent all departments with local guest account solutions).

**Sample of Current Guest Account Systems**

- Residential and Student Service Programs
    - Separate accounts for "co-habitants" (family members of residential contract holders)
    - Separate accounts for conference guests
- Boalt School of Law
    - Separate accounts for guest faculty and their support staff
    - Separate accounts for conference guests
- Educational Technology Service
    - Separate guest account system for bSpace site access (over 100s of sites)
- IST
    - Standalone system for managing guest wireless access (AirBears)
    - Need solution for guest CalShare accounts
    - Will need guest access solutions for MediaHub project

A campus-wide guest access management system would allow the retirement of these stand-alone departmental guest systems.

3. While the campus has made significant headway in standardizing and centralizing authentication, the campus still lacks a standard approach to user authorization. The campus does not have any defined institutional roles which translate into access rights for a set of business systems, nor any simple way to create centrally accessible user groups based on access rights. Access is still managed largely on an application-by-application basis with a variety of approaches. Some applications check the CalNet managed campus directory service (LDAP) for specific user attributes before granting access to a particular service. Other applications maintain local application-specific authorization tables based on defined roles, and the process by which these roles are requested, approved, and administered is often manual.

A handful of applications have been integrated into the System Access Request Application, which provides a more central system for requesting access to core campus business systems, but which is not intuitive to use, is costly to maintain and integrate with, and still results largely in a manual process for provisioning and de-provisioning access to business systems.

A. Describe the solution that is being proposed to meet the identified need(s).

Identity and access management offers great promise as a key component to standardizing, streamlining, and securing user lifecycle management and access to electronic resources on campus (and even beyond through federated identity management).
A robust, central identity and access management infrastructure would deliver a variety of efficiencies across campus, by

- eliminating local user account stores currently used to manage guest access
- increasing productivity by streamlining access request and approval processes and getting users on board quicker
- reducing labor costs by automating many access management steps currently handled manually
- reducing the risk of security breaches by better managing access rights

Identity and access management sits at the intersection of user experience, business process, identity data, and campus business systems. Improvements in identity and access management require engagement and participation from key stakeholders in each of those areas. Coordinated effort among stakeholders has the potential to yield considerable campuswide savings. Disjointed efforts will result in wasted resources.

B. Describe the alternate approaches you evaluated in the process of developing this proposal and why those alternatives were not selected.

There are a variety of technical solutions to the problem of centralizing access management. The CalNet team is currently investigating them. The alternative to not providing a central access management tool is to continue the current method of implicit access management where central campus IT makes available a fairly wide set of information about people (subject to data proprietor approval) and application owners query that data to determine whether or not to grant access. Such an approach makes it impossible to audit access rights centrally and for users and administrators to view the complete set of access rights for any given user.

## III. IMPACT AND STRATEGIC ALIGNMENT

A. Describe how the proposed solution aligns with the OE goals:

- Reduce administrative costs and enable the campus to direct more resources to teaching and research
- Advance an effective and efficient operating environment
- Instill a culture of continuous improvement that leads to high quality performance and outcomes

After a lengthy engagement with the campus in 2006, the Burton Group concluded that improvement in identity and access management would streamline operations and reduce operational costs. With coordinated effort and investment, the campus can achieve a central, secure, streamlined access management system which handles access request and approval for well-defined campus roles, updates identity data from source systems, creates and removes access rights across multiple campus systems, and provides centralized audit and reporting for access rights (see attached diagrams).

The current SARA system is very costly to maintain and it is cost-prohibitive for applications to integrate with it. A more modern access request system would expand the capability of campus to implement central access management. Such a centralized system would integrate well with grouper and is a likely pre-requisite to other OE resource requests where users

would be granted roles with access to privileged information, such as the Advising Toolkit request and the online performance evaluation proposal.

Efficiency Improvements that can be achieved by eliminating SARA include:

- Eliminates significant staff time in Controller's office currently spent administering access rights
- Eliminates lost productivity due to length of time it takes to get someone "in the system" with the correct access rights
- Reduces the security risk (and cost of potential security breaches) introduced by the reliance on manual processing given that the current system includes no automated way to de-provision access when employees leave or change roles
- Eliminates ongoing maintenance costs for the SARA application (servers, system administration, DBA, Web Applications)
- Greatly reduces the costs of establishing consistent access management approach for new systems

A central access management system would also allow the retirement of stand-alone guest access systems, yielding cost saving in departments across campus.

Finally, a central access management system is a critical component to a number of proposed OE projects which will require a mechanism for granting specific users access to sensitive data, including the Hyperion Planning project, Advising Toolkit, and the proposed student and staff portals.

B. Identify any other anticipated benefits in implementing the proposed solution.

In addition to eliminating the current inefficiencies noted above, a central access management system would reduce the cost and streamline the process for integration new applications which required central access request and approval workflow.

C. Identify the risks of not implementing the solution.

- At present, the cost of adding new applications to SARA is prohibitive, so departments are forced to develop and support stand-alone electronic or paper-based access request and approval processes.
- The continued reliance on manual provisioning and de-provisioning of access rights is error prone and subjects the university to significant risk of allowing unauthorized access to resources, for example failing to deprovision access when users leave the university or change jobs during their tenure.

D. Describe the constituency that is intended to benefit from the proposed solution (e.g. students, faculty, staff, 1-many units)

A central access management system would benefit the entire campus as it could be used to manage access for students, staff, and faculty to campus business applications.

E. Describe the extent to which this proposed solution is a collaborative effort either within campus or with external partners.

Any access management system requires active participation from the staff that manages the system itself (the CalNet team) and the business functional owners and technical staff that manage the system for which access is being granted. Centralizing access management for applications with multiple,

complex roles, such as enterprise HR and financial systems, requires considerable business process analysis and technical implementation effort.

If central access management were implemented along with other OE initiatives, like the advising toolkit, significant staff contributions from the initiative group would be required, primarily with regards to documenting access management requirements, reviewing UIs and workflow, and testing integrations before production migration.

This proposal includes a Roles Engineering effort as part of the first phase of the project. The existing Identity and Access Management Steering Committee, which includes representation from key campus stakeholders, can be leveraged to define and develop campus-wide roles. In the past, the committee has discussed whether or not the new Career Compass job mappings could be used to standardize access rights for specific positions. The committee has repeatedly concluded that job functions are still not standard enough across departments, even for positions with the same Career Compass mapping, for job classifications to work well as a base point for bundling access rights. The Roles Engineering effort would look at common bundles of access rights that are granted to certain types of employees, particularly bundles related to large, enterprise business applications.

F. If applicable, describe how the proposed solution may enable additional projects to be considered.

As noted above, central access management would likely be needed for any project which requires the granting of privileged access to some users, such as the advising toolkit project, online performance management, online financial planning, etc.

G. What is the impact of the proposed solution on the existing systems and processes? Does it eliminate the need for existing systems and processes?

A central access management system would eliminate the need for the current SARA system and would eliminate the need for many stand-alone departmental guest access systems. A central access management solution would also eliminate and estimated 2 hours of staff time for every new hire and every termination.

H. What is the impact on the proposed solution on the workload?

| Profile/Impact in hours | Current Workload | 1-time workload requirement per integration at least initiallly | Ongoing workload requirement |
|---|---|---|---|
| Student | | | |
| Staff | | * Roles Engineering (first two years) – see budget worksheet for detail | $235,000 annual for project management, business analyst, and technical staff time (see budget worksheet for detail) |
| Faculty | | | |

## IV. WORK PLAN AND PROPOSED SOLUTION DESIGN

A. Provide a statement of:

- Deliverables — results the solution must deliver to achieve the stated objectives.
- Constraints — factors that may limit the options for providing the solution (*e.g., an inflexible deadline*).

The CalNet team already has a long list of guest access integrations that they are working on. The pace

at which we can move through these depends on the resources at our disposal. Also, the CalNet team is evaluating technical implementation options as we are leaning against continuing our investment in Sun Identity Manager (Oracle Waveset). As we have not yet settled on the technology we wish to implement, we are keeping our access management integrations as simple as possible for now.

B. Provide a work plan for the proposed solution with high-level steps to complete the solution, including timeline. (Try to limit your plan to no more than seven steps.)

| | MILESTONE | TIMELINE |
|---|---|---|
| 1. | Review Access Management Technology Solutions | Fall 2011 |
| 2. | Begin Role Engineering | Fall 2011 |
| 3. | Choose new product or product suite for future access management efforts | Winter 2011 |
| 4. | Implement access management for new OE projects | Spring 2011 |
| 5. | Complete Role Engineering | Summer 2012 |
| 6. | Add SARA applications as resources permit and as departmental staff are available to conduct their side of the integration | Spring/Summer 2012 |

C. What are the data requirements for the proposed solution?

Detailed information about roles and access rights for applications that wish to integrate with the central access management system. Detailed understanding of how the application/system performs authorization and where authorization data needs to be provisioned.

D. What are the technical requirements for the proposed solution?

Implementation and ongoing maintenance of central access management system, including all associated infrastructure. Detailed documentation or roles and permissions as described above. Use of standard authorization stores that the central access management system can provision to.

E. What are the greatest risks for the proposed solution and the plan to reduce or eliminate the risks.

| | RISK | MITIGATION PLAN |
|---|---|---|
| 1. | Marketplace for commercial access management solutions is very volatile. Could invest in a tool that is later abandoned/acquired | Choose a suite of products based on open standards and available as open/community source as much as possible. |
| 2. | Cost to integrate with central access management system will still be seen as too costly | Provide some funding to subsidize costs of early integrations, as future integrations should be less costly once we build a code base. |
| 3. | | |
| 4. | | |
| 5. | | |

F. How does the proposed work plan allow for evaluation and course correction to ensure the outcomes meet the campus needs?

Each access management integration is a discrete project and gives everyone time to evaluate the effort and outcome and make improvements.

## V. CHANGE MANAGEMENT

A. What is the change management plan to successfully implement the outcomes of the proposed solution?

We will form a implementation team that will include CalNet staff members as well as campus application developers and campus data providers. The project will be led by a project manager with assistance from a business process analyst.

B. What incentives and/or disincentives are proposed to influence behavioral changes necessary for the successful outcome of the proposed solution?

People will be naturally incented to use a system which is more intuitive than the current SARA. A number of campus departments have requested improved central access management, so there is a ready pool of campus departments willing to engage with central service providers.

C. Who has been identified as the change leaders and implementers to carry out the changes necessary for the successful outcome of the proposed solution?

The CalNet Identity and Access Management team will serve as primary change leaders, but strong engagement and leadership will also be needed from those systems that integrate with the central access management system.

As mentioned above, many campus departments have already committed resources to engaging in this effort, particularly those departments seeking improve access request and approval for guest/affiliate accounts. The campus Guest Account Taskforce, formed by the Identity and Access Management Steering Committee, identified a number of campus departments who manage local guest account systems which would be able to retire those systems if a central solution were available.

A number of campus departments have also expressed a strong willingness to commit resources to integrating their local systems/applications with a central access management system, including the Enterprise Data Warehouse team.

Because each central access management integration will require commitment of resources from the CalNet team as central service provider, as well as the local application team, there is a limit to the number of integrations that can be tackled at any given time. Sequencing of access management effort will need to be discussed in relation to priorities for OE projects. The CalNet team could likely focus on 2-3 priority OE projects during the Fall of 2011, such as the Hyperion Planning project and the Academic Commons. Once access management was implemented for a few key OE projects , the CalNet team could begin work with the applications which currently use SARA.

## VI. FUNDING MODEL AND BUDGET

A. Could the proposed solution move forward with partial funding? If yes, describe the revised scope, including the associated savings impact.

The project could move forward with partial funding, but the pace would be slowed, and may not meet

the requirements of other OE requests that will rely on access management solutions.

B. What is the plan for sustainable funding to support ongoing operations of the proposed solution?

The CalNet team has estimated an ongoing resource need of $235,000 annually for support of a central access management service, including project management, business analyst, technical staffing and infrastructure. This expense could be offset by charging campus departments a fee for integrating with the central access management solution, though such a fee may discourage integration and result in a continuation of inconsistent and insecure access management practices on campus.

C. Please download and fill out the OE Resource Request Budget Template and follow the instructions on the first worksheet in the workbook to complete the budget ant line descriptions. Include both completed sheets with the Resource Request.

Detailed budget estimates are provided in the accompanying financial spreadsheets.

## VII. ASSESSMENT PLAN

Please use the table below to detail your metrics.

| METRIC CATEGORY | SPECIFIC MEASURE | MEASURE BASIS | DATA COLLECTION METHOD | DATA COLLECTION FREQUENCY | FUNCTIONAL OWNER OF DATA COLLECTION | LARGER GOAL TO WHICH METRIC RELATES |
|---|---|---|---|---|---|---|
| ***EXAMPLES:*** | | | | | | |
| ***FINANCIAL PERFORMANCE*** | | | | | | |
| *1 Reduction in average price of office supplies* | *Avg price* | *Per item* | *Look at vendor catalogs* | *Quarterly, first day of each quarter* | *Procurement Director* | *Overall reduction of 15% in average price of office supplies* |
| ***OPERATIONAL PERFORMANCE*** | | | | | | |
| *1 Reduction in average processing time per transaction* | *Avg person-hours required* | *Per transaction* | *Survey of transaction processors* | *Semi-annually* | *Director of Billing* | *Reduction of 20% in average transaction processing time* |
| | | | | | | |
| **FINANCIAL PERFORMANCE** | | | | | | |
| **1. Eliminate** costs associated with SARA | Line items for SARA eliminated from IST bill | Per month charges | Review IST Bill | Annual | CalNet team | Migration to central access management system for efficiency and reduced risk |
| **2 Eliminate costs associated with local guest account systems** | Departments systems for guest account | Per month charges | Review of departmental expenses | Annual | Departments managing local guest access | Migration of all user accounts to central authentication |

| | | | | | | |
|---|---|---|---|---|---|---|
| | management retired | | | | systems | and authorization systems to eliminate redundancies and reduce risk |
| **3 Reduction in time to on-board and off-board staff** | Survey admin staff before and after regarding time to on/off-board | Reduction in reported time to on/off-board | Survey results | Pre and Post-integration for key applications | CalNet team and local department | Greater efficiency in on/off-boarding process |
| | | | | | | |
| **OPERATIONAL PERFORMANCE** | | | | | | |
| **1 Ability to deploy new applications in a secure, timely, and efficient manner** | Time and cost required to establish access management for a new application | Central and departmental staff time required | Reported hours to complete integration | After each integration | CalNet team and local department | Protect access to data, improve ability to deploy campus-wide systems efficiently |
| **2** | | | | | | |
| | | | | | | |
| **PRODUCT / SERVICE QUALITY** | | | | | | |
| **1** | | | | | | |
| **2** | | | | | | |
| | | | | | | |
| **EMPLOYEE SATISFACTION** | | | | | | |
| **1 Improvements in new employee/new faculty satisfaction** | User satisfaction with on-boarding experience | Reported improvements in satisfaction for new staff/faculty | Survey results | After hire | Human Resources | Reduced time to productivity for new staff |
| **2** | | | | | | |
| | | | | | | |
| **CUSTOMER SATISFACTION** | | | | | | |
| **1** | | | | | | |
| **2** | | | | | | |
| | | | | | | |
| **PUBLIC RESPONSIBILITY** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **1** | Reducing risk to user's by better protecting confidential records | Fewer systems rely on manual access rights management | Periodic audit of selected campus systems | Annual | Audit | Minimize risk that the campus will experience a data breach |
| **2** | | | | | | |
| | | | | | | |
| **SUPPLIER PERFORMANCE** | | | | | | |
| **1** | | | | | | |
| **2** | | | | | | |