UCSB Audit and Advisory Services

Internal Audit Report

UCTrust Compliance Review

February 6, 2014

Performed by:
Tony Samer, Protiviti
Jason Brucker, Protiviti
Scott Nakamura, Protiviti
Joe Murrell, Protiviti
Dominic Zumbo, Protiviti
Antonio Manas-Melendez, Senior Auditor

Approved by:
Robert Tarsia, Director

Report No. 08-14-0003

This page intentionally left blank.

University of California, Santa Barbara

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
SANTA BARBARA, CALIFORNIA 93106-5140
Tel: (805) 893-2829
Fax: (805) 893-5423

February 6, 2014

To: Elise Meyer, Director of Infrastructure
Enterprise Technology Services

Matthew Dunham, Associate Director
Identity, Directory & Provisioning Services
Enterprise Technology Services

Re: **UCTrust Compliance Review**
Audit Report No. 08-14-0003

As part of the 2013-14 annual audit services plan, Audit and Advisory Services conducted a compliance review of UCSB's participation in UCTrust, the UC systemwide identity management system. The primary purpose of the project is to ensure that University of California, Santa Barbara (UCSB) is in compliance with essential UCTrust requirements. The compliance work plan for this project was developed in consultation with the systemwide audit unit of the UCOP Office of Ethics, Compliance and Audit Services, and will be made available for systemwide use.

Our review found that the University is not fully compliant with UCTrust requirements. There are also opportunities for improvements in UCTrust oversight and communication, and for formalizing documentation relating to roles and responsibilities and procedural guidance.

Detailed observations and management corrective actions are included in the following sections of the report. The management corrective actions provided indicate that each audit observation was given thoughtful consideration and positive measures have been taken or planned to implement the management corrective actions. The cooperation and assistance provided by Enterprise Technology Services and departmental personnel during the review was sincerely appreciated. If you have any questions, please feel free to contact me.

Sincerely,

Robert Tarsia
Director
Audit and Advisory Services

cc: Chancellor Henry Yang
Senior Associate Vice Chancellor Marc Fisher, Administrative Services
UCSB Audit Committee
Senior Vice President and Chief Compliance and Audit Officer Sheryl Vacca

Enterprise Technology Services
Denise Stephens, Interim CIO
Brian Richard, Director, Enterprise Planning and Architecture
Maria Ayllon, UCPath Project Manager

UC Office of the President - Office of Ethics, Compliance and Audit Services
Matt Hicks, Systemwide Audit Director
Greg Loge, Systemwide IT Audit Manager

UCSB Audit and Advisory Services
UCTrust Compliance Review
Audit Report No. 08-14-0003

PURPOSE

The primary purpose of this review was to determine whether University of California, Santa Barbara (UCSB) is in compliance with essential UCTrust requirements, as outlined in the *UCTrust University of California Identity Management Federation Service Description and Policies*. This audit is part of the fiscal year 2013-14 audit services plan of UCSB Audit and Advisory Services.

SCOPE, OBJECTIVES AND METHODOLOGY

The scope of the review included current UCSB UCTrust processes and practices. The project objectives included:

- Developing a compliance work plan based on the *UCTrust University of California Identity Management Federation Service Description and Policies* (*UCTrust Service Description and Policies*). The compliance work plan for this initial UCTrust compliance review, developed in consultation with the systemwide audit unit of the University of California Office of the President (UCOP) Office of Ethics, Compliance and Audit Services, will be made available for UC systemwide use.

- Completing the audit procedures outlined in the compliance work plan.

- Determining whether UCSB is in compliance with essential UCTrust requirements, including those related to governance, roles and responsibilities for participation and administration, and technical and service level standards required.

To accomplish our objectives, we:

- Reviewed and analyzed *University of California* (UC) policies and procedures related to identity and access management and security, including Business and Finance Bulletin IS-11, *Identity and Access Management* (BFB IS-11); Business and Finance Bulletin IS-3, *Electronic Information Security* (BFB IS-3); and Business and Finance Bulletin IS-10, *Systems Development and Maintenance Standards* (BFB IS-10).

- Reviewed and analyzed the *UCTrust Service Description and Policies*.

- Developed a draft compliance work plan based on the *UCTrust Service Description and Policies*.

- Interviewed stakeholders involved with UCTrust and the employee onboarding process, including Enterprise Technology Services (ETS) personnel and the business officers of two UCSB departments, Psychological & Brain Sciences and Music.

- Performed detailed audit procedures in key areas detailed in the draft compliance work plan, including obtaining and reviewing:

    - Documentation, including the UCTrust Charter, select policies from the Identity, Directory & Provisioning Services group, and UC and campus new hire / rehire processes.

- Configuration settings, which define or describe appropriate security requirements, including passwords and encryption methods used, and technical specifications, including protocols, formats, and software required.
- Attributes, which define or describe a person's membership to UCTrust and includes the entitlements or abilities granted to the person.

.

We also determined whether there are appropriate UCTrust governance mechanisms in place to help ensure compliance with minimum UCTrust requirements and service levels.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

UCTrust and the UCTrust Federation (collectively known as UCTrust) was a unified identity and access management (IAM) project mutually agreed upon in 2004 by IT leaders from the UC campuses. In March 2007, the *UCTrust University of California Identity Management Federation Service Description and Policies* document was developed to establish guidance on the principles, governance, participants, responsibilities, minimum requirements and service levels, audit requirements, and technical specifications for UCTrust and UCTrust compliance. The document provided a basis for a unified identity and access management infrastructure for the UC system, an infrastructure that enables authorized campus individuals to use their local campus electronic credentials to gain access, as appropriate, to participating services (Resource Providers) throughout the UC system.

The UC campuses, medical centers, and national laboratories can join UCTrust by registering with the UCTrust Federation Administration. Members included in UCTrust are also members of the InCommon Federation (InCommon) by default, since UCTrust is considered a subset of InCommon. InCommon is a nationwide higher-education identity management federation focused on creating a common framework for collaborative trust in support of research and education. InCommon makes sharing protected online resources easier, safer, and more scalable with the increased use of digital resources and services. InCommon also enables cost-effective, privacy-preserving collaboration among participants[1].

A fundamental principle of UCTrust is that participating campuses provide authoritative and accurate identity information about individuals in their campus community. Further, UCTrust provides a framework for uniform business practices that establish electronic credentials and maintain individual identity information. UCTrust is based on industry standard technologies (including Shibboleth) and a common set of identity attributes (e.g., user name, campus affiliation, etc.) and identity management practices. It also establishes the minimum standards (or levels of assurance) for the identification, registration, and authentication of those campus community members who require access to resources with higher-level requirements. A level of assurance describes the policies and practices that have been applied and can be used by the Resource Providers to determine their confidence in the identity information they receive.

[1] InCommon Federation website - Frequently Asked Questions @ http://www.incommonfederation.org/docs/guides/faq.html).

Table 1	Key Identity Management and UCTrust Terms
Term	**What it Means**
Identity and Access Management	*Refers to the processes and procedures used to administer and safeguard an individual's authentication, authorization, and privileges within or across system and enterprise boundaries to increase security and productivity, while decreasing cost, downtime, and repetitive tasks.*
UCTrust	*Unified identity and access management infrastructure for the UC system that enables authorized campus individuals to use their local campus electronic credentials to gain access to participating services (Resource Providers) throughout the UC system.*
UCTrust University of California Identity Management Federation Service Description and Policies ***(UCTrust Service Description and Policies)***	*Document developed in 2007 to establish guidance on the principles, governance, participants, responsibilities, minimum requirements and service levels, audit requirements, and technical specifications for UCTrust.*
UC IT Leadership Council (ITLC)	*Acts as the governing body of UCTrust by providing direction for its operational policies, technology, and procedures, based on input it receives from the UCTrust Workgroup and UCTrust Federation Administration. ITLC is comprised of Chief Information Officers and/or representatives of executive IT leadership at each UC campus.*
UCTrust Federation Administration	*Used in this report to describe the group comprised of the Identity Management leads at each UC campus (also known as the UCTrust Workgroup) that shares and addresses operational issues with UCTrust.*
Resource Providers	*The campus organizational units that manage electronic information resources that have been registered with UCTrust. They are also responsible for the secure operation of their services.*
Credential Providers	*The campus organization units that manage electronic identity information and provide identity information and authentication services for their campus. They are also responsible for the campus's repository of information about the members of its community.*
Shibboleth	*The software used by InCommon that provides and transmits information between the Resource Provider and the service provider. The information is bundled using security assertion markup language (SAML) and the data contains the assertion (e.g., UCTrust assertion level). Shibboleth leverages the local authentication system the University supports and handles the exchange of identity information among identity management systems and participating applications in UCTrust.*

The minimum requirements and service levels for Credential Providers and Resource Providers to comply with UCTrust include:

- *Credential Providers*
  - Identification and registration processes for issuing electronic credentials (e.g., user ID and passwords) to individuals.
  - Authentication process to verify possession of credentials within each session.
  - Implementing the common set of identity attributes and publishing/exchanging attribute information with participating Resource Providers and other Credential Providers.
  - Provide a help desk function for problem resolution.
  - Provide documentation that describes compliance with responsibilities and requirements.
- *Resource Providers*
  - Applications that utilize UCTrust must be compliant with University policies.
  - Responsible for the security of their services.
  - Address appropriate usability concerns prior to registration with UCTrust Federation Administration.
  - Ability to exchange attribute information with other Credential Providers and Resource Providers.
  - Provide a help desk function for problem resolution related to the application.

The *UCTrust Service Description and Policies* also stipulate that Credential Providers and Resource Providers will be audited periodically to provide independent assurance of compliance with the applicable policies, principles, and requirements of UCTrust. Audits of Credential Providers are required at least once every two years, and audits of Resource Providers are required at a frequency to be determined by the IT Leadership Council (ITLC). These audits may be performed either by UC internal audit departments or other qualified independent auditors. Audit results are to be reported to the ITLC and shared with Resource Providers and Credential Providers, upon request.

The benefits of UCTrust include:

- Enables cost-effective, privacy-preserving collaboration among participating UC campuses, facilitating the sharing of protected online resources and eliminating the need for Resource Providers to maintain separate password-protected accounts.

- Supports individuals' access to protected resources by allowing Resource Providers to make decisions about granting access to their resources based on authoritative information offered by the individual's campus regarding that individual's status of local privileges.

- Offers a high level of security by utilizing strong controls over secure access channels. This high level of security also provides a secure mechanism for ensuring privacy in the exchange of identity attributes.

At UCSB, the Associate Director, Identity, Directory & Provisioning Services, has been working to implement the essential UCTrust requirements and is a member of the UCTrust Federation Administration.

SUMMARY OPINION

Our review found that the University is not fully compliant with UCTrust requirements. There are also opportunities for improvements in UCTrust oversight and communication, and for formalizing documentation relating to roles and responsibilities and procedural guidance.

Audit observations and management corrective actions are detailed in the remainder of the report.

DETAILED OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS

A. Organizational Oversight and Communication

Our interviews with stakeholders confirmed that the UCTrust Federation Administration is comprised of the identity management leads at each UC campus, and is managed collectively. Since responsibility and authority for managing UCTrust is not clearly assigned to a single administrator or manager, there is the potential for ineffective management and oversight, as well as inefficiencies. We were informed during our audit fieldwork that the Office of the President is aware of the challenges and has hired an Identity Management lead; this individual may become the UCTrust administrator with a significant level of responsibility and authority for UCTrust operations. In the absence of these changes, the UCTrust Federation Administration or the Office of the President should consider selecting a current member of the UCTrust Federation Administration or hiring an individual to be the administrator.

The draft UCTrust Work Group Charter states that a Chair and Co-Chair (chairpersons) will lead and oversee the UCTrust Work Group. Many of the responsibilities of the chairpersons appear operational and include:

- Convening the UCTrust meetings and coordinating activities, action items, and deliverables across the UCTrust membership.
- Meeting regularly with the IAM Lead in the UCOP Enterprise Architecture team to plan UCTrust discussions; preparing recommendations for the IT Architecture Group (ITAG), other subcommittees, and ITLC; and collecting input from across the UC system to influence decisions related to IAM across UC.
- Coordinating the review and evaluation of requests to UCTrust, framing/scoping recommendations for next steps (proceed with or forward to appropriate parties), and presenting to ITAG and/or ITLC for concurrence and/or guidance.
- Administering the UCTrust wiki, including structure and content, and ensuring that UCTrust members and others have appropriate access and permissions.
- Facilitating engagements with other UC subcommittees and working groups who may inform and/or participate in UCTrust work efforts.

The UCTrust Federation or UCOP should consider expanding these responsibilities to ensure that there is appropriate oversight to ensure effective and efficient management of UCTrust. Areas to consider include provisions to oversee UCTrust participants, completing the required documentation, and overseeing the maintenance of a repository for description of requirements and UCTrust attributes. Additionally, the chairpersons could assist with problem resolution between Credential Providers and Resource Providers.

Our interviews also identified a concern that the audit frequency for Credential Providers is not well understood. Although the *UCTrust Service Description and Policies* clearly state the audit requirement, it does not appear that all Credential Providers have read or fully understood this requirement, or that the audit requirement has been complied with systemwide. The UCTrust Federation Administration should more clearly develop, document, and communicate UCTrust audit requirements, including the specific responsibilities to the UCTrust Credential Providers and Service Providers at each UC campus.

Management Corrective Actions

UCSB has essentially no direct control over the issues detailed above, as the operation of the UCTrust Federation is within the purview of UCOP. We will present these deficiencies to our Chief Information Officer, who may bring them to the UCOP IT Leadership Council for discussion and possible engagement.

Audit and Advisory Services will follow up on the status of this issue by August 31, 2014.

B. Formal Documentation

The results of our stakeholder interviews identified a need for better formal documentation related to UCTrust roles and responsibilities and procedural guidance. At the time of our fieldwork, the responsibilities of the UCTrust Credential Providers and Service Providers had not been formally documented as required by Sections 8.1 and 8.2 of the *UCTrust Service Description and Policies*. The UCTrust Credential Provider at UCSB understood his responsibilities as inherent to his role in identity management, and complies with campus security policies. Although there is overlap between these responsibilities, there are some responsibilities that are specific to the UCTrust Credential Provider. For example, there is a requirement to provide documentation describing ongoing compliance with the UCTrust policies, principles, and requirements; the UCTrust Credential Provider confirmed that he is currently is not in compliance with this responsibility (see discussion under C. Compliance with UCTrust Requirements, 3. UCTrust Registration, below). Also, since UCSB currently does not host a UCTrust application, a Resource Provider is not applicable. However, if/when UCSB hosts a UCTrust application; the University should consider documenting the Resource Provider responsibilities.

Additionally, our interviews with stakeholders indicated that there are no documented procedures to provide guidance on the rules for governing release and use of UCTrust attributes in Section 9.1.1.9 of the *UCTrust Service Description and Policies*. Specifically, some attributes have different levels of sensitivity than others based on who is consuming this information (inside versus outside the UCTrust Federation), and this is managed on an ad hoc basis. The UCSB Identity Management team obtains approval from the data owner prior to releasing any information, which increases inefficiencies and decreases the consistency of information released and used. For example, the UCSB Identity Management team must get authorization from Student Affairs to release any student identification information, which may or may not be consistent with the protocols that are followed by another campus department to release similar employee or contractor identification information.

The UCTrust Credential Provider at UCSB indicated this was completed on a case-by-case basis. To provide more consistency across UCTrust, the UCTrust Federation Administration should consider formalizing procedures to provide guidance on sensitivity levels and level of assurance required for UCTrust attributes.

Management Corrective Actions

As stated in response to section A, issues of service documentation and central release policies also fall within the operation of the UCTrust Federation as managed by UCOP and aren't within the scope of UCSB to correct ourselves. Instead, we can escalate these deficiencies to UCOP via our IT leadership chain-of-command for discussion.

Audit and Advisory Services will follow up on the status of this issue by August 31, 2014.

C. Compliance with UCTrust Requirements

1. Verification of Identity

Our interviews with stakeholders identified that UCSB is not consistently verifying the identity of individuals by using a government-issued photo ID, as required by Section 9.1.1.2 of the *UCTrust Service Description and Policies*. The University's official hiring process, which includes completion of the Form I-9[2], does not specifically require verification of an individual's identity via a government-issued photo ID. Other forms of identification (or combinations of other forms) may be used to verify the identity of an individual.[3] Meetings with stakeholders did indicate that it is uncommon for an individual not to present government-issued photo ID to verify identity.

We also understand the Associate Director, Identity, Directory & Provisioning Services, is planning to develop a process to identify the list of individuals whose identity was not verified with a government-issued photo ID. When this process is complete, a member of the Identity, Directory & Provisioning Services team will verify the individual's identity with a government-issued photo ID.

2. Attributes and Configurations

At the time of our fieldwork, stakeholders indicated that there were attributes and configurations that have not been completed or published in accordance with UCTrust requirements. Attributes contain data to provide assurance related to how well the Credential Provider knows the person is who they say they are. The assurance value is published by UCTrust to ensure the individual is trustworthy. Currently, UCSB complies with UCTrust by publishing attribute values for individuals. Individuals at UCSB have a value of "null", which indicates that there is trust that the person is affiliated with UCSB, but not that the individual meets the UCTrust requirements detailed in Section 9 of the *UCTrust Service Description and Policies*. (Individuals meeting these requirements would have an attribute value of "basic.") Based on interviews with stakeholders, there is concern that it is unclear whether it is acceptable that full UCTrust compliance is applicable to a subset of UCSB individuals, or whether it should apply to all individuals at UCSB. As an example, students may not meet UCTrust requirements by definition and should have an attribute value of "null". The UCTrust Federation Administration should consider providing guidance on the UCTrust "basic" level of assurance and if that level of assurance is required for all individuals at the University.

[2] Form I-9 must be completed by employers to document verification of identity and employment authorization of each new employee (both citizen and noncitizen) hired after November 6, 1986.
[3] Form I-9 includes a list of acceptable documents that an employer may use to verify a person's identity. Not all forms of identification listed contain a photo. Examples of acceptable documents and combinations of documents that may not include a picture are voter registration card with Social Security Account Number card, or a voter registration card with Certification of Report of Birth issued by the Department of State (Form DS-1350).

In addition, UCSB has not implemented all of the requirements identified in Sections 9.1.1.5 and 9.1.1.6 of the *UCTrust Service Description and Policies*, since these requirements are not enforced to access services managed by UCTrust. These include the ability to confirm existing records of an individual (e.g., email, phone number, or mailing address) and multi-factor authentication[4].

Table 2	**Comparison of UCTrust Common Identity Attributes and UCSB Attributes**	
Attribute	**UCTrust Common Identity Attribute**	**UCSB Attribute**
eduPersonScopedAffiliation	Yes	Yes
eduPersonPrincipalName	Yes	Yes
eduPersonEntitlement	Yes	Yes
eduPersonTargetedID	Yes	No
sn	Yes	Yes
givenName	Yes	Yes
displayName	Yes	Yes
Mail	Yes	Yes
transientId	No	Yes
cn	No	Yes
UCnetID	No	Yes
UCTrustAssurance	No	Yes
UCTrustCampusIDShort	No	Yes
ucsbCampusID	No	Yes

We understand the UCTrust requirements were published in the *UCTrust Service Description and Policies* in 2007 based on assumptions and technologies that existed at that time. We also understand that an audit at each campus may be completed to determine compliance with UCTrust requirements. The UCTrust Federation Administration should considering reassessing and updating UCTrust specifications based on advancements in technologies and common themes and feedback from the audits at each campus,

3. UCTrust Registration

UCSB has not registered with the UCTrust Federation Administration in accordance with Section 5.1 of the *UCTrust Service Description and Policies*. This section requires UCSB's ITLC Representative and the Credential Provider or Resource Provider to jointly certify ongoing compliance with the UCTrust policies, principles, and requirements. The Associate Director, Identity, Directory & Provisioning Services has not completed and submitted the form to the UCTrust Federation Administration, since he understands that UCSB is currently not in compliance. Additionally, based on discussions with personnel at other UC campuses, he is not aware of any UC campus that is currently in compliance with all UCTrust requirements.

[4] Multi-factor authentication is used to verify/confirm the identity of a user. The authentication factors relate to something only the user knows (e.g., password, PIN, pattern); something only the user has (e.g., ATM card, smart card, mobile phone); and something only the user is (e.g., biometric characteristic, such as a fingerprint).

Once UCSB is in compliance with the requirements outlined in the *UCTrust Service Description and Policies*, the UCSB ITLC representative and Credential Provider/Service Provider should complete the certification of compliance form and submit it to the UCTrust Federation Administration.

Management Corrective Actions

C.1. Verification of Identity

We will indeed be developing a process by which we can perform photo ID verification to meet UCTrust Basic requirements around identity proofing. However, until we have clarity on the scope of individuals for whom we need to meet this level of assurance, we can't design this process. We will work with the UCTrust Federation Administration to get clarity on this question, and design and implement this process once we have clear direction.

C.2. Attributes and Configurations

As noted above, we will work with UCTrust Federation Administration to better understand the populations for which certain attributes are meant to apply. It's our belief that some of these attributes are not strictly required for all University populations. If we verify this is the case, we will exhort the federation management to update the specification accordingly. Otherwise we will ensure the necessary attributes are applied universally.

C.3. UCTrust Registration

Once we recognize that that we are indeed compliant with all of the conditions and requirements detailed in the UCTrust Service Description and Policies document, we will formally register our service accordingly. We believe we should not perform registration until we know we are fully compliant.

Audit and Advisory Services will follow up on the status of this issue by August 31, 2014.