UNIVERSITY OF CALIFORNIA, BERKELEY

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

SANTA BARBARA • SANTA CRUZ

AUDIT AND ADVISORY SERVICES
Tel: (510) 642-8292

611 UNIVERSITY HALL #1170
BERKELEY, CALIFORNIA 94720-1170

August 25, 2021

Catherine P. Koshland
Interim Executive Vice Chancellor and Provost

Marc Fisher
Vice Chancellor
Administration

Interim Executive Vice Chancellor and Provost Koshland and Vice Chancellor Fisher:

We have completed our audit of UC Berkeley's CalNet Identity Access Management as per our annual service plan in accordance with the Institute of Internal Auditors' *Standards for the Professional Practice of Internal Auditing* and the University of California Internal Audit Charter.

Our observations with management action plans are expounded upon in the accompanying report. Please destroy all copies of draft reports and related documents. Thank you to your staffs for their cooperative efforts throughout the audit process. Please do not hesitate to call on Audit and Advisory Services if we can be of further assistance in this or other matters.

Respectfully reported,

Jaime Jue
Director

cc: Associate Vice Chancellor and Chief Information Officer Jenn Stringer
Chief Information Security Officer Allison Henry
Senior Vice President and Chief Compliance and Audit Officer Alexander Bustamante
Associate Chancellor Khira Griscavage
Associate Vice Chancellor and Controller Michael Riley

AUDIT AND ADVISORY SERVICES

CalNet Identity Access and Management Audit
Project No. 20-737

August 25, 2021

Prepared by:

Deloitte
Systemwide Co-Sourced Provider of Internal Audit Services

Reviewed by:

Jennifer E. Jones
Associate Director

Approved by:

Jaime Jue
Director

University of California, Berkeley
Audit and Advisory Services
Identify Access Management Audit

Table of Contents

OVERVIEW

Executive Summary

Identity and Access Management IAM) is used to define, identify, authenticate and manage user roles and their associated access privileges related to systems, technologies and data. With both the increase in regulatory requirements and the sophistication of cybersecurity attacks, the importance of robust IAM controls and processes has been highlighted as critical to protecting valuable and confidential data assets (e.g., research data, intellectual property, personally identifiable data and financial data). Weaknesses in IAM controls and processes could result in unauthorized access and a compromise in the confidentiality, integrity, and availability of University data and systems. As an industry, higher education institutions have incurred various such breaches which have resulted in financial losses and fines, reputational detriment, loss of leading research information, non-compliance with regulatory and legal requirements, and non-availability of critical systems and data.

There are various components of a successful IAM program that involve policy, procedural, and technical considerations, and that can be managed on a centralized or decentralized basis depending on the needs and structure of the organization. A key underpinning of the campus IAM program is a centralized (single sign-on) authentication and authorization system, known as CalNet, that is used to enable access to key campus enterprise systems by more than 70,000 students, faculty, staff, affiliates, visiting scholars, sponsored guests, and alumni ("users").

Based on our work performed, internal controls appear adequate to address the core risks assessed as part of this internal audit; however, we identified instances of supporting controls not being designed and implemented effectively or controls not always operating effectively. Specifically, we noted opportunities to enhance oversight and protocols related to the provisioning of access at the application and supporting system layers to help mitigate risk more broadly and ensure the overall objectives of an IAM program are achieved.

Internal controls needing improvement are summarized in the next section. Management agrees with the observations and has provided management responses that we believe will adequately mitigate the noted risks.

Source and Purpose of the Audit

The objective of this review was to evaluate the design, implementation, and operating effectiveness of internal IAM utilized by the campus and assess their alignment with established University policies, procedures, and leading practices. The audit was performed as part of our approved fiscal year 2020 audit plan.

Scope of the Audit

The period in scope for the audit was July 2019 through June 2020 and our review primarily focused on controls in place to support the management of user identity, authentication and access privileges related to the centralized CalNet services. Internal controls relating to the provisioning of user access to specific enterprise systems and applications served by CalNet are managed on a decentralized basis at the application level, and their design and effectiveness was not directly assessed as part of our audit work. Audit procedures performed included

- Reviewing campus IAM governance, including policies, procedures, and guidelines, and assessing availability and completeness of documents, as well as alignment with leading practices[1] and broader University policies and guidelines.

- Interviewing key personnel to develop an understanding of the design of current IAM control activities and processes, including
  - tools and technologies used;
  - roles and responsibilities;
  - Windows Domain administration;
  - user authentication parameters, including password management and multi-factor authentication (MFA);
  - CalNet account and access privilege provisioning, including use of generic and special accounts;
  - CalNet account and access privilege deprovisioning, including grace period management and account expiry;
  - user activity logging and monitoring; and
  - periodic vulnerability scanning and testing.

- Performing sample-based testing to assess operating effectiveness of controls over account administration (students, faculty/staff, affiliates, visiting scholars, sponsored guests, and alumni) for users provisioned and deprovisioned from July 1, 2019 through June 30, 2020, including identity creation, baseline access privilege provisioning and user access deprovisioning.

- Identifying opportunities for improvement within the IAM processes to strengthen internal controls and further mitigate risk.

[1] For the purposes of this review, policies and procedures were assessed for the comprehensiveness and level of detail of guidance provided. This included determining if the following key processes, and associated controls, have been documented in a clear manner and supports consistency of control performance: account administration, user access and authentication, local and remote access protocols, and vulnerability management.

Work performed was limited to the specific activities and procedures described above. As such, this report is not intended to, nor can it be relied upon to, provide an assessment beyond those areas specifically reviewed. Audit planning, fieldwork, and reporting was conducted by the staff of Deloitte, systemwide co-source provider of internal audit services. Their work was reviewed and approved by Audit and Advisory Services management to ensure consistency with guidance outlined in the UC Internal Audit Manual.

Background Information

The CalNet Identity and Access Management team within the Office of Information Services and Technology provides the campus with a centralized authentication and authorization system for campus enterprise systems, including the Berkeley Financial System, Student Information Systems, and the UC human resources and payroll system, UCPath, among others. These services can be broken down into five primary categories.

- Identity Data Services (IDDS): CalNet curates identity data from several University systems of record. Identity Data Services represent a suite of technology solutions that allow campus programmers with complex needs to consume identity data to make access control and resource provisioning decisions.
- Access Services: CalNet maintains Single Sign On (SSO) services that allow campus community members to use the same account to access many different online applications. Access Services are consumed by application owners who need to leverage SSO to manage access to their applications.
- Account Services: Account Services provide the tools that individuals need to manage and maintain their digital access credentials and accounts.
- User Support Services: User Support Services provides authorized University technology support staff with the tools they need to be able to diagnose and remedy access errors.
- Internal Services: CalNet requires flexible, scalable infrastructure components to move and maintain large amounts of identity data. Internal Services are consumed or maintained by CalNet to facilitate the delivery of the service portfolio.

University departments use CalNet services to validate users to access departmental applications, obtain authoritative information about users, and for public directory service and lookups. User access within the applications are administered and managed locally by the departments.

Key policies governing campus IAM programs derive from systemwide policies, primarily *BFB-IS-3: Electronic Information Security* and *BFB-IS-11: Identity and Access Management*.

Summary Conclusion

Based on our work performed, internal controls appear adequate to address the core risks assessed as part of this internal audit; however, we identified instances of supporting controls not being designed and implemented effectively or controls not always operating effectively. Specifically, we noted opportunities to enhance oversight and protocols related to the provisioning of access at the application and supporting system layers to help mitigate risk more broadly and ensure the overall objectives of an IAM program are achieved.

Internal controls needing improvement are summarized in the next section. Other areas identified as best practices were verbally communicated to management. Management agrees with the observations and has provided management responses that we believe will adequately mitigate the noted risks.

SUMMARY OF OBSERVATIONS & MANAGEMENT RESPONSE AND ACTION PLAN

User Administration – Application Layer

Observation

User administration at the application layer is not granted or monitored centrally through CalNet. Application owners are individually responsible for determining access structures (roles, segregation of duties, etc.) and performing ongoing user access reviews. This presents the risk of user access protocols and risk tolerance being applied inconsistently, with a limited view (and ability to apply additional layers of security) centrally. Although applications owners can use the CalNet Active Directory (CalNet AD) affiliations to determine access, currently the use is limited.

In addition, there are currently no formal, centralized controls in place for enforcing or monitoring the deprovisioning of a terminated user at the application layer. It is possible for user accounts to continue to have access at the application layer after termination, if their access is not manually revoked by the application owner(s) because applications may not fall under the CalNet domain.

Where user access is not consistently maintained, the risk of users having access privileges beyond the minimum necessary and/or the performance of inappropriate activity is increased. Abuse of such access may result in the compromise of sensitive data, non-adherence with compliance requirements, financial loss and reputational loss for the University.

It is recognized that management are currently investigating potential tools to help standardize user administration at the application layer. Such tools may also be used to apply additional policies/layers of security when desired (e.g., applying rulesets around the types of access that may be granted to each user base [i.e., students, faculty, staff] for certain categories of applications).

Management Response and Action Plan

This finding relates primarily to the lack of a centralized Access Management system. The Information Security Office and Enterprise Operations are investigating potential vendor solutions. In order to better understand the marketplace and cost for viable solutions, an RFI for Access Management software was completed and recommendations presented to the CIO. During the FY22 fiscal year, options will be evaluated, and a funding proposal will be developed for a campuswide access management solution. Implementation of a solution will be dependent on receiving necessary funds, for both software licensing and staff FTE to support the solution.

User Administration – Active Directory Domain Administrator Access

Observation

The processes for provisioning and deprovisioning Active Directory (AD) domain administrator access may not consistently follow the formally documented processes in place. In addition, no formally documented policy is in place for processing exceptional terminations of administrator accounts.

Formally documented and consistently enforced user administration procedures help to determine consistency and provide an audit trail if the need to review such activity arises. This risk is partially mitigated due to the fact that all such access must be approved by the Director and that AD domain admin access is restricted to a small number of individuals. However, leading practice would suggest that all such access requests are formally documented and approved prior to gaining such privileged access.

Management Response and Action Plan

A process for provisioning and deprovisioning will be documented and published by the Windows Server group by August 2021.