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 3, 2023

To: Distribution

Re: **IT: UCPath Separation of Duties Management**
Audit No. 08-23-0002

We have completed a review of UCPath separation of duties management as part of the 2022-23 annual audit services plan. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*. Enclosed is the report detailing the results of our work.

We sincerely appreciate the cooperation and assistance provided by Administrative Services, Business & Financial Services, Academic Personnel, Human Resources, and Enterprise Technology Services personnel during the review. If you have any questions, please contact me.

Respectfully submitted,

Ashley Andersen
Director
Audit and Advisory Services

Enclosure

Distribution

Business & Financial Services
Jim Corkill, Associate Vice Chancellor and Controller
Kimberly Ray, Associate Director of Controls

Academic Personnel
June Betancourt, Director

Human Resources
Lisa Romero, Human Resources Interim Director

Office of the CIO
Josh Bright, Chief Information Officer
Emilio Valente, Chief Information Security Officer
Matt Erickson, Director for IT Program Management

Enterprise Technology Services
Manny Cintron, Director of Application and Technology Services

cc: Chancellor Henry Yang
David Marshall, Executive Vice Chancellor
Chuck Haines, Vice Chancellor - Chief Financial Officer
Garry Mac Pherson, Vice-Chancellor, Office of the Vice Chancellor for Admin Services
UCSB Audit Committee
Alexander Bustamante, Senior Vice President and Chief Compliance and Audit Officer

This page intentionally left blank.

UC SANTA BARBARA
Audit & Advisory Services

Audit Report

IT: UCPath Separation of Duties Management

February 3, 2023

Performed by:

Antonio Mañas-Melendez, Associate Director
Anne-Sophie Gatellier, Senior Auditor

Approved by:

Ashley Andersen, Audit Director

Report No. 08-23-0002

EXECUTIVE SUMMARY

OBJECTIVE

The primary purpose of this audit was to evaluate the processes in place to manage separation of duties within the roles assigned to campus personnel in the UCPath system and to identify inadequate practices managing UCPath roles. Our review particularly assessed whether:

- Role provision requests are properly documented and approved.
- Separation of duty controls prevent users from preparing and approving their own transactions.
- Existing access rights are periodically reviewed and access is revoked after termination.
- Adequate training and/or guidance is available.

CONCLUSION

Based on the results of the work performed within the scope of the audit, we found:

- Inconsistencies in the support documentation required by Department Security Administrators (DSAs)[1] to request role changes, including tracking formal manager approvals.
- Opportunities to improve the process to revoke access to UCPath after the termination of personnel or when campus personnel move to a new position where there is no need to have access. Departments have been inconsistently aware of their responsibility to request access removals, as is required by BFB-IS-3: *Electronic Information Security* (IS-3 Policy).
- Lack of monitoring active users and assigned roles within the departments.
- Opportunities to reevaluate refresher training alternatives for end-users and develop guidance for DSAs.

[1] See background section for definition.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. ROLE-BASE ACCESS CONTROL AND AUTHORIZATION PROCESS

OBSERVATION

Our evaluation of the process for granting access to UCPath has highlighted a need to clarify the required support documentation to request provision of roles, including tracking formal manager approvals. Additionally, we found inconsistencies in the process to remove access, particularly in the case of a change of position within UCSB. There are also opportunities to reevaluate refresher training alternatives for end-users[2].

Authorization and Support Documentation

We found that the support documentation required by DSAs to process UCPath role provision requests varies across departments, and, in some departments, provision requests and departmental approvals are not consistently documented.

We reviewed the process for granting UCPath roles to end-users in five departments and selected 15[3] role requests, processed in fiscal year 2021-22, to verify whether support documentation and preapprovals were properly retained. We found that all DSAs use the ServiceNow[4] ticketing system to document the request, and all role provision requests were approved by a department manager. However, we noted that five DSAs did not have the adequate support documentation in nine role requests[5]. Additionally, these nine requests were approved by managers that were not the direct manager of the employees granted with new roles, as is suggested by Business and Financial Services (BFS) best practices *Guidelines for Managing System Access*[6].

In addition, we verified whether all universal and central access requests in the audit period were approved by the UCPath Steering Committee at UCSB (the Steering Committee). Our review shows that the approval process was appropriately conducted for all 32 universal and central accesses requested during the audit period:

- 30 universal / central access requests were approved by the Steering Committee.
- Two requests were initially rejected. Roles were requested again later as departmental role and provisioned as such.

In terms of timeline, we identified that 96% of the requests submitted in fiscal year 2021-22 have been approved and closed within seven days, and 100% within ten days. Considering the absence of timeline requirements and the absence of urgency in the regular access process, we consider this timeline reasonable.

[2] End-user is a person who ultimately uses or is intended to ultimately use a computer application or system.
[3] Three samples for five DSAs.
[4] Online ticket system that allows users to report and track IT-related service issues and/or requests.
[5] DSAs explained that they are the knowledgeable person in terms of access to request, and did not need additional documentation.
[6] For more information on the Guidelines for Managing System Access, see the Background section.

Finally, we verified if the 93 individuals who submitted access tickets over fiscal year 2021-22 were active DSAs. We identified two individuals who are not DSAs and had submitted three requests that granted 23 roles. We were informed that both of them are ServiceNow fulfillers, and not DSAs. The local procedure was updated during the audit to ensure a manual check is performed.

Table 1 shows the number of tickets received in fiscal year 2021-22 to add access to UCPath, per type of access.

Table 1 Type of Access Requests Over FY 2021-22

Type of Access	Access Requests
Departmental	334
Central / Universal	32
Total	**366**

Source: ETS, and auditor analysis.

Transactional User Training Requirements

End-users are required to complete training in order to be granted transactional roles. However, there are no refresher training requirements.

We reviewed 17 roles requests, processed in fiscal year 2021-22, to verify whether users granted with the new access had completed the required training:

- In seven cases, no training requirements were necessary because they only requested inquiry roles[7].
- In six cases, the user completed the training, including one exception process approved by the UCPath Organizational Manager. This exception process is documented in ETS procedure.
- In four cases, the user received training prior to the new curriculum[8]. Even though receiving a refresher is not required by policy, it could be beneficial to evaluate alternatives to allow transactional users refresh their knowledge, especially for users who received training before the new curriculum.

Role Assignment

Our review did not identify any user who was inappropriately provisioned with their role. However, guidance to the DSAs and controls performed by the DSAs to ensure the appropriateness of access provisioned could be enhanced.

While analyzing ServiceNow requests, we came across five tickets that did not specify the roles requested:

[7] Training is not required when the role is inquiry only.
[8] For more information on the training requirements, see Background.

- Four tickets requested cloning access from a different user, or from a similar previous position in a different unit.

- One ticket asked ETS to clarify what the roles should be for a Management Services Officer.

ETS usually checks that the access requested is appropriate for the user even though it is a DSA's responsibility to verify the appropriateness of role requests[9].

We assessed that departments with end-users granted with a role to process direct retros[10] required this role to perform their responsibilities. We selected all departments with more than ten end-users provisioned to process direct retros and confirmed with DSAs that all the end-users needed this role.

Guidance to Understand Roles

Table 2 UCSB Entrée Roles, and Availability of Description

UCSB Entrée Roles*	Number of End-users*	View Only Role	Description Available
WFA Inquirer	546	Yes	Yes
Patent Inquiry	546	Yes	No
PFA Inquirer	504	Yes	Yes
TAM Hiring Manager	**436**	**No**	**No**
WFA Initiator	427	No	Yes
BSA Reports	425	Yes	No
Budget Reports	420	Yes	No
WFA Reports	411	Yes	No
Case Manager	389	No	Yes
PFA Reports	384	Yes	No
PFA Initiator	384	No	Yes
BSA Inquirer	326	Yes	Yes
Budget Inquirer	298	Yes	Yes
WFA Approver - All	279	No	Yes
PFA Approver - All	257	No	Yes
Budget Manager	201	No	Yes
Work Study Inquiry	179	Yes	No
Person Org Inquiry	102	Yes	No
Other Roles	< 60	**N/A**	No

Source: ETS, HR website, and auditor analysis.
* As of July 20, 2022.

[9] ETS informed us that they check for security appropriateness and provide guidance. As long as the request is not for Central or Universal roles, ETS will fulfill the request made by the DSA.
[10] A direct retro, or salary cost transfer, is an immediate transfer of account balances made to correct accounting/funding errors which have already been paid.

Human Resources has published a description of ten UCSB Entrée roles[11], including the main roles that allow making changes in the system. However, eight of the 18 frequently assigned roles are not documented. Specifically, the transactional role TAM Hiring Manager and seven view-only roles are not described, although they have been provisioned to more than 100 end-users. Documenting roles would help DSAs to understand the meaning of the UCPath roles they request. Table 2 shows the number of users per UCSB Entrée role, and whether a description is available.

We found that there is no documented guidance available on campus to match positions with their most common roles. The high level of decentralization at UCSB makes it difficult to create a one-size-fits-all mapping of positions versus roles.

Our interviews of five DSAs show that most of them learned their role on the job, without any pre-requisite or training on how to request roles, which roles, and on separation of duties. DSAs are mostly not aware of any guidance[12] on their role and responsibilities, which puts the responsibility of confirming the access needed on ETS. This is not compliant with the IS-3 Policy.[13]

Termination of Employee Access

We found opportunities to improve the process to revoke access to UCPath after the termination of personnel or when campus personnel move to a new position where there is no need to have access.

Departments in the scope are not always aware of their responsibility to request access removals of employees leaving the department, as is required by IS-3 Policy. When users are separated from the University, UCPath access are automatically deactivated with their UCSB NetID. However, users who transfer to another campus do not automatically have their access deactivated, and DSAs do not verify if the access was deactivated. ETS resets all prior UCPath departmental roles when a DSA requests access to a new department for an employee.

Access removals are initiated either by the department or when ETS is informed of a position change within UCSB, and concludes that former roles have to be removed. Our interviews show that only two DSAs out of five proactively request access removal when the user leaves their position. The other three DSAs have not included it in their process and rely on ETS or the next manager to address the removal needs. However, ETS removes access on the department's request only.

We reviewed the list of all 746 active UCPath users, and found 20 who were not active employees as of July 20, 2022. More specifically:

- Two employees had been terminated in September and December 2021[14].

[11] UCSB Entrée roles are local functional roles,

[12] Guidelines for managing system access were updated on the BFS website in August 2022, and address campus systems managed by DSAs.

[13] UC Policy IS-3 states that this is the responsibility of the workforce manager to review access rights annually and removing access that is no longer needed.

[14] These employees were campus transfers, and have their roles for the new campus. This issue is a reporting issue and these users cannot use their roles for UCSB transactions.

- 18 users were inactive due to being on leave or work break. Although there is no specific guidance on access for users in these situations, the Steering Committee does not expect users on a leave to lose their access in a systematic way.

In addition, we asked five DSAs to review the list of their users to verify it was up-to-date. We identified two active employees who had access they were not supposed to have. Their roles were removed during the audit. Table 3 shows the number of transactional users and their status as UCSB employees.

Table 3 Active UCPath Transactional Users

Employee Status	Active UCPath Users*
A - Active	726
L - Unpaid Leave	7
P - Paid Leave	10
T - Terminated	2
W - Work Break	1
Total	**746**

Source: ETS, and auditor analysis.
* As of July 20, 2022.

RECOMMENDATION

We recommend UCPath Steering Committee update the UCPath System Role Descriptions to guarantee descriptions of the most provisioned roles are included. Descriptions related to roles will provide comprehensive information to help DSAs identify the appropriate roles.

MANAGEMENT RESPONSE

UCPath Steering Committee will update the description of the most provisioned UCSB Entrée roles available. Descriptions related to roles would provide comprehensive information to help DSAs identify the appropriate roles.

Audit and Advisory Services will follow up on the status of these issues by April 28, 2023.

2. SEPARATION OF DUTIES

OBSERVATION

Conflicting Roles

The Steering Committee does not consider it necessary to develop a local separation of duties matrix because the application has been designed to prevent users from preparing and approving their own transactions: One transaction would require the participation of at least two users to be fully executed.

Additionally, provisioning some users with roles they might not need to perform their main responsibilities, such as preparer and approver roles for some specific transactions, has been

justified as a back-up solution in case of absence or unexpected turn-over. Campus departments have a reduced number of personnel, and even minor personnel availability issues could make it impossible to process UCPath transactions in some departments. We confirmed that UCPath does not prevent a DSA from assigning the preparer and approver roles to the same user.

We performed a limited testing analyzing 2,756 direct retro transactions created and approved over fiscal year 2021-22 to determine whether these transactions were processed and approved by the same user. In all 2,756, the preparer and the approver were different users.

Periodic reviews[15] of the UCPath UCSB roles have been performed by UCPath Center. As a result, potential conflicting roles based on the UCPath Center's matrix have been reported and addressed locally. This includes a response approved by the Steering Committee.

3. MONITORING

OBSERVATION

Access Review

We noted that DSAs do not have adequate tools to perform periodic reviews of existing access rights, and departments do not perform these reviews, as is required by IS-3 Policy.

The departments interviewed have no process in place to review the access on a regular basis, and they are not aware of a report to assist them is this task. ETS informed us that a UCPath role would allow the DSA to review their users whenever deemed necessary. However, this review would be user by user, and would show UCPath roles that might be difficult to understand for the DSAs. Besides, three DSAs interviewed out of five stated they do not keep track of their users and their roles. One DSA has an outdated list of roles requested when UCPath was implemented[16], but they are not maintaining it, nor do they have a process in place to review users on a regular basis. Having access to a report that lists the users and roles related to the department would allow the departments to perform a review of the roles provisioned in the system, on a regular basis.

RECOMMENDATION

We recommend the UCPath Steering Committee, in cooperation with Enterprise Technology Services, evaluate the possibility of providing DSAs with a user account report, including the access provisioned, in order to assist them in the monitoring of their users.

MANAGEMENT RESPONSE

The UCPath Steering Committee, in cooperation with Enterprise Technology Services, will evaluate the possibility of providing the DSAs with a user account report, including the access provisioned, in order to assist them in the monitoring of their users.

Audit and Advisory Services will follow up on the status of these issues by April 28, 2023.

[15] We have not considered it necessary to include an assessment of roles in the scope of this audit because UCPath Center periodically performs this assessment.

[16] UCPath was implemented at UCSB in 2018.

GENERAL INFORMATION

BACKGROUND

Separation of Duties (SoD)[17]

According to NIST, separation of duties refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time).

IS-3 Policy

IS-3 Policy requires that workforce managers consider the principle of SoD when designing and defining job duties. Workforce managers must:

- Implement methods and controls in their area of responsibility that, to the extent feasible and appropriate, separate duties among workforce members so that the roles of requestor, approver, and implementer are independent.

- Establish effective oversight of activities and transactions. When functions cannot be separated, adequate administrative oversight or other compensating controls must be in place to mitigate identified risks.

- Implement segregation of duties where duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. No one person has control over all aspects of any financial transaction.

- Make sure that transactions are authorized by a person with delegated approval authority when the transactions are consistent with policy and funds are available.

Guidelines for Managing System Access[18]

Business and Financial Services (BFS) has published local guidelines to describe responsibilities related to requesting, approving, and managing access to systems. The user's supervisor's responsibilities include but are not limited to:

- Recognizing that an employee's job duties require the need to view system information or to execute transactions.

- Determining which system role and its corresponding permissions are appropriate for the employee's job duties.

- Considering whether granting system access will conflict with system access for other assigned duties.

[17] Source: National Institute of Standards and Technology (NIST) website.
[18] Source: UCSB Business and Financial Services website.

- Submitting a request to the DSA specifying why system access is needed and that the access is approved.

- Notifying the DSA when an employee's role or access to a system should be deleted due to separation from the University or a change in job duties.

- Maintaining records that document changes to access rights and their related approvals.

The DSA's responsibilities include but are not limited to:

- Based on general knowledge of the employee's job duties, considering whether the requested role(s) and corresponding privileges are appropriate.

- Ensuring requests are approved by the employee's supervisor or manager.

- On a periodic basis but no less frequently than once a year, reviewing system access reports with supervisors and managers.

Department Security Administrator (DSA)

The DSA is a department-level role that has the approval rights to grant departmental permissions to users within UCPath. Although there is no campuswide guidance specific to UCPath access management, BFS released new guidelines stating that the manager is responsible for submitting "*a request to the DSA specifying why system access is needed and that the access is approved*"[19]. Main responsibilities are:

- Record all accountability delegations identified by the organizational head or designee.

- Provide appropriate access for all on-line preparers and the prescribed reviewers of a department's on-line transaction activity.

- Update the official record of accountability delegations each time a change is required such as when an individual leaves, is hired, or their responsibilities change.

- Ensure that the official record of accountability delegations is secure from unauthorized changes.

- Maintain a current back-up copy of the official record of accountability.

UCPath Training[20]

UCPath training is provided for UCSB employees who perform specific transactional tasks in UCPath, including initiators, approvers, and inquiry-only users. Transactional users are those with roles allowing them to perform transactions in UCPath that are not related to their personal employee status. These roles are provisioned in addition to standard roles provisioned to all UCSB employees. A series of web-based and instructor-led courses provides each UCSB learner with the necessary skills and training to ensure system

[19] The guidelines for managing system access were updated on the new BFS website launched on August, 2022.
[20] Source https://www.ucpath.ucsb.edu/training.

proficiency. Participants must complete all of the required courses before receiving access to UCPath.

ETS verifies that initiators, approvers, and budget managers complete the training prior to being provisioned with their roles, in compliance with UCSB training requirements. The current curriculum was released in November 2019, and includes a variety of topics that were not systematically covered in previous courses. However, users who completed previous courses are not required to complete the new curriculum.

SCOPE

The scope of our audit included the review of:

- Access management processes:
    - For a sample of units, we:
        - Interviewed the Department Security Admins (DSAs).
        - Obtained available departmental documentation related to role mapping and access tracking.
        - Verified whether the current list of users and their UCPath roles for these units was still relevant.
        - Selected a sample of UCPath access requests over fiscal year 2021-22 and assessed their compliance in terms of documentation, approval, and training requirements.
    - Verified whether current UCPath users completed the mandatory training.
    - Verified whether current UCPath users are active UCSB employees.
    - Verified whether direct retro transactions over fiscal year 2021-22 were requested and approved by a different user.
- Monitoring and DSA training processes. In particular, we:
    - Verified whether all current DSAs are active UCSB employees.
    - Verified whether DSAs receive training related to their role and responsibilities.
    - Reviewed periodic reports from UCPath Center and assessed how they are handled locally.
    - Verified whether roles currently provisioned are consistent with the ETS role mapping.
    - For a sample of users with a role related to direct retros, verified with the DSAs whether these roles are relevant.

- Verified whether roles rejected by the Steering Committee had been provisioned.
- Verified whether removal requests had been properly processed.

UCPath Center performs audits, including separation of duties twice a year, and provides the results to each location. Our review does not include a configuration review.

CRITERIA

Our audit was based upon standards as set forth in the UC and UCSB policies, best practices, and other guidance relevant to the scope of the review. This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

In particular, we reviewed:

- University of California BFB-IS-3: *Electronic Information Security*
- Business and Financial Services *Guidelines for Managing System Access*
- Departmental UCPath Access Request Workflow
- Universal UCPath Access Request Workflow

AUDIT TEAM

Ashley Andersen, Audit Director
Antonio Mañas-Melendez, Associate Director
Anne-Sophie Gatellier, Senior Auditor