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 15, 2022

To: Distribution

Re: **IT: Separation of Duties**
Audit Report No. 08-22-0001

We have completed a review of separation of duties in campus financial systems as part of the 2021-22 annual audit services plan. The objective of this audit was to identify potential separation of duties gaps in critical campus systems. The review 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 the personnel of Business and Financial Services, Enterprise Technology Services, and Department Security Administrators 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

Office of Budget and Planning
Kerry Bierman, Associate Vice Chancellor
Michael McGrogan, Budget Director

Office of the Chief Information Officer (CIO)
Shea Lovan, Interim Chief Information Officer
Kip Bates, Associate Chief Information Security Office

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

cc: Chancellor Henry Yang
Chuck Haines, Associate Chancellor for Finance and Resource Management
UCSB Audit Committee
Alexander Bustamante, Senior Vice President and Chief Compliance and Audit Office

This page intentionally left blank.

UC SANTA BARBARA
Audit & Advisory Services

Audit Report

IT: Separation of Duties

February 15, 2022

Performed by:
Antonio Mañas Meléndez, Associate Director
Gifty Mensah, Senior Auditor

Approved by:
Ashley Andersen, Audit Director

Report No. 08-22-0001

EXECUTIVE SUMMARY

OBJECTIVE

The objective of this audit was to assess the separation of duties in a sample of campus financial systems by assessing whether:

- Access requests are properly documented and approved.
- Roles are periodically reviewed and restricted after employee termination.
- Critical and conflicting roles are properly restricted and monitored.
- Workflows are operating as expected.
- Reports for monitoring events are available.

The review was limited to the following five financial applications on campus:

- Cashnet
- Transfer of Expense (TOE)
- Transfer of Funds (TOF)
- Travel (TRVL)[1]
- Form 5 Online/Disbursement (DISB)[1]

CONCLUSION

Based on the results of the work performed within the scope of the audit, we found controls that ensure separation of duties between the preparer and approver roles in each of the financial applications reviewed. However, there are opportunities for improvement in the following areas:

- Support documentation to justify access control changes and the business need to grant conflicting or privileged roles.

- Monitoring tools and reports to identify potential issues and events.

- Training needs for Department Security Administrator (DSAs).

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

[1] These systems have been replaced with the new system, Concur in February 2022. Concur was not reviewed in this audit.

OBSERVATIONS, RECOMMENDATIONS, AND RESPONSES

1. ROLE-BASE ACCESS CONTROL AUTHORIZATION PROCESS

OBSERVATION

Our evaluation of the process for granting access to user accounts, and modifying privileges in financial applications managed by ALLN02[2] within Gateway Management Console (GMC), has highlighted a need to evaluate a consistent process to document authorization requests. Additionally, we found control gaps in the process for assigning and removing roles of users, more specifically:

- Informal and inconsistent documentation of role assignments and modifications.
- DSAs assign roles to themselves.
- Employees who have separated from the University with active user accounts.

Support Documentation

We found that the support documentation of authorization requests varies across departments, in some cases, it is limited or nonexistent.

The DSA is a department-level role that has the approval rights to grant permissions to department users within many of the ALLN02 applications, such as TOE, TOF, TRVL, and DISB. During the audit, we reviewed the process for assigning roles to users for a sample of seven DSAs and found that there is no consistency in the tools used to manage authorization requests, more specifically:

- Two DSAs use the ServiceNow[3] ticketing system to document the request and obtain approval from users' supervisors.

- One DSA uses an onboarding access request form which is completed by department heads.

- Four DSAs rely on verbal discussions and email communication with users and department directors on role requests.

Additionally, we tested 15 role modifications from January 2020 to July 2021, consisting of three samples for five DSAs. We noted no or limited support documentation supporting authorization requests, more specifically:

- Four out of five DSAs sampled did not have documentation to support the roles they assigned or unassigned to users. They explained that the role requests were either discussed verbally with supervisors or via email correspondence. They could not provide the email correspondence.

[2] ALLN02 –This Is a role management system for Espresso applications. These are the campus legacy financial applications that were moved off the mainframe unto the Gateway Management Console.
[3] ServiceNow - It is an online portal that allows users to report IT-related service disruptions or service requests. It uses a ticket system to track the requests.

- One provided an access request form that was completed by the user's department head. We consider this form acceptable.

Approval Process

DSAs and administrators can assign permissions to themselves in the ALLN02.

During the review, we assessed whether users for all applications in the ALLN02 have approval rights to assign their own permissions. From January 2014 to September 2021, we identify 125 users who assigned their own permissions in the ALLN02 systems within this period:

- 120 users were DSAs who assigned permissions to themselves in the various applications over the period. This list includes 20 former DSAs and 100 active DSAs. Some DSAs who assigned the permissions to themselves explained that it was their personal decision to assign the role to help them perform some tasks for their departments.

- Two were system administrators in the GMC whose roles can do any function including assigning/unassigning roles to themselves. Three were campus security administrators (CSAs)[4] who have elevated privileges and often assign themselves various roles in order to troubleshoot a ticket. We consider these cases acceptable.

Termination of Employee Access

We found opportunities for improvement in the procedure to revoke access to ALLN02 applications and Cashnet after the termination of personnel or when campus personnel move to a new position where there is no need to have access.

We tested 10 users in Cashnet and all user accounts in ALLN02 and found 133 active users accounts of employees who have exited the university as of September 30, 2021. More specifically:

- One Cashnet user was no longer an employee as of September 30, 2021. We were informed that this application is not integrated with the Campus Identity Manager and relies on password expiration.

- 132 users with active accounts in ALLN02 had separated from the University. Five of them have active DSA roles. However, access is tied to users' UCSB NetID and it is only restored when the NetID is activated. We were informed that a DSA and a CSA remove access only when they receive a request to do so even though sometimes they know someone has left the University.

2. SEPARATION OF DUTIES

OBSERVATION

Our test has highlighted that DSAs could require additional guidance to properly assess the

[4] CSA has the responsibility of assigning the DSA role to users in the ALLN02.

business need of users with conflicting roles, such as administrator roles or a combination of administrator roles and transactional roles.

UC policy[5] states that *"University assets/data must be safeguarded from loss or unauthorized access and use: Access to any forms or on-line systems that can be used to alter financial balances must be restricted to qualified and competent employees who require such access to perform their University duties"*

During our review, we obtained a report of all users and their roles in the Cashnet, TOE, TRVL, DISB (Form 5 Online), and TOF systems. We mapped out the roles to identify users in the categories explained below:

Administrator Roles

The number of users with administrator roles in some of the applications could be considered excessive because some users would not need to have administrator roles to perform their duties.

We assessed the appropriateness of the number of users who have administrator privileges in each of the systems to ensure the role is limited to people who need to have access. We found the following:

- The Cashnet system has two users with administrator privileges. We consider this number acceptable.

- The TOF system has 11 users with functional administrator privileges. We were informed that the administrator rights in this system are included in a transactional role called TOF-APR (final approval of transfers) which is limited to staff of the Budget Office. The administrator role has limited functionality and we consider it a low risk to pair this role with operational roles. However, the department confirmed that four users (two of which have retired) do not need access and could be removed.

- The TOE system has six users with an administrator role. The department confirmed that two users do not need to have this role.

- Five users in the TRVL system have at least one of the two administrator-type roles. Three of these combined this role with two transactional roles (Travel Approver or Travel Voucher Enterer). DISB system has four users with an administrator role and three of them have an additional three transactional roles (Disbursement Accounting Approver, Accounting Preparer, and Accounting Stamp Receiver). Concur has replaced the TRVL System and the authorization model is different.

Conflicting Roles

We noted that there is currently no risk of a lack of separation of duties because these applications prevent the preparer from approving their own transaction. However, we found user accounts with conflicting roles. For example, the Preparer/Submitter and Approver/Releaser roles or having an administrator role combined with other transactional

[5] BFB-BUS-10: Principles of Accountability with Respect to Financial Transactions.

roles. Any new functionality or modification of the application could potentially circumvent the control in the code and create a lack of separation of duties.

We confirmed that the GMC doesn't prevent a DSA from assigning the Preparer/Submitter and Approver/Releaser roles to the same user, but the application prevents the preparer from approving their own transaction.

Additionally, we tested this control by analyzing processed vouchers from August 2020 to September 2021. In all transactions for the various applications, different user accounts performed the Prepare and Approval roles. However, it could be convenient to perform periodic reviews of users with conflicting roles to determine the need and to limit the number.

Restricted roles

Some users have a role that is restricted to a specific department to which they are not assigned.

We reviewed the list of roles that are restricted to certain departments on campus and confirmed whether individuals outside the departments have been assigned those roles.

We found that, in the TRVL application, a role named "TRVUNRES" is restricted to users from Business and Financial Services. However, we identified 10 users who are not in Business and Financial Services but have been assigned this role.

Unnecessary Roles

Some users could have more roles than needed for their job.

We reviewed whether documented users' roles are consistent with the principle of least privilege for the sampled applications. We found three users (one in the TRVL application and two in the DISB system) could have more permissions than needed to perform their day-to-day duties. As mentioned before, both systems have been replaced by Concur which uses a different authorization model.

In all other applications reviewed, we did not find any users we would consider as having excessive roles.

3. REPORTS AND MONITORING

OBSERVATION

Our work found a need to promote the use of existing monitoring tools to easily identify inappropriate activities and events. We found that existing tools and reports in the ALLN02 application could be underutilized by DSAs.

During the review, we verified whether there are periodical reports or functionalities to monitor roles and users' activities and if these reports are available to the DSA or departments. Examples of these include reports to identify:

- Users with conflicting roles / administrative roles.
- Submitting and approval of same transactions.

- Active user accounts assigned to personnel who have exited the university.

These reports or functionalities help to easily flag events or identify inappropriate actions in the system. Specifically,

- There are no such monitoring reports in the Cashnet system. There are audit logs for modifications of transactions. The system also records the last login and last failed login. The department could evaluate the need for incorporating some of the above monitoring reports.

- The ALLN02 applications have two kinds of reporting tools available in the management section of the system: User role report, and Assignment report. The reports have filters that could produce useful information about users' activities and roles. However, these reporting functionalities could be underutilized by some DSAs. Additionally, there are also audit logs for role modifications and transactions in the system.

  We were informed that this application uses multi-factor authentication and could prevent concurrent and other unusual logins.

4. TRAINING

OBSERVATION

Our review found a need to update the training manuals for DSAs and to evaluate training alternatives to help DSAs in understanding their role.

The CSA assigns a DSA role to an individual when a request is made in ServiceNow. The request form requires MSO and department head email addresses. An automatic email is sent to these email addresses on the request, but it does not request their confirmation or approval of the request.

During the audit, we noted the following from interviews conducted with seven DSAs:

- There is no formal training for DSAs on their role.

- Some DSAs have no knowledge of the roles or what the actual permissions mean and are not in a position to determine whether a role request is right for the user.

- Most DSAs do not question a role request. They assign what is requested and rely on the department to determine the appropriateness of the request of the functional user.

Additionally, we reviewed the two manuals, ALLN02 Financial System DSA Authorizations Functions Guide, and ALLN02 Self Training Guide for DSAs, that are given to DSAs when they are first assigned the role. We noted that these are technical documents that provide useful information on how to use the tools such as how DSAs can use the GMC to access the ALLN02 functions, assignment logs, and basic assignment reports available for monitoring.

However, we found that these manuals could be updated to include the following:

- Procedures to ensure sufficient documentation and tracking of role requests and

approvals.

- Demonstrate the need for ensuring that roles are assigned based on necessity and to the appropriate individuals.

- Outline certain conflicting roles that DSAs could look out for or should avoid.

- Procedures requiring DSAs to review user roles periodically.

- Procedures on how to use the monitoring reports on the management screen.

RECOMMENDATION

We recommend Business and Financial Services, with the support of Enterprise Technology Services:

- Evaluate whether implementing a ticket system or a digital access request form could make the process more efficient.

- Update current manuals and provide guidance to DSAs on:

    - Documenting and tracking access requests. The support documentation should include justification of business needs and adequate approvals. Exceptions when necessary, such as DSA roles assignations, should be properly documented and approved.

    - How to utilize reporting functionalities to identify information such as restricted roles, users with conflicting roles, and inactive user accounts and the need to review such reports periodically to identify inappropriate activity.

    - Exit practices such as revoking access and disabling user profiles after they leave the department or the University.

MANAGEMENT RESPONSE

Business and Financial Services, with the support of Enterprise Technology Services, will

- Evaluate whether implementing a ticket system or a digital access request form could make the process more efficient.

- Update current manuals and provide guidance to DSAs on:

    - Documenting and tracking access requests. The support documentation should include justification of business needs and adequate approvals. Exceptions when necessary, such as DSA roles assignations, should be properly documented and approved.

    - How to utilize reporting functionalities to identify information such as restricted roles, users with conflicting roles, and inactive user accounts and the need to review such reports periodically to identify inappropriate activity.

- Exit practices such as revoking access and disabling user profiles after they leave the department or the University.

Audit and Advisory Services will follow up on the status of these issues by May 31, 2022.

GENERAL INFORMATION

BACKGROUND

Separation of duties (SoD) is a security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud. The most widely adopted SoD model requires separation between authorization (AUT), custody (CUS), recording (REC), and verification (VER)[6].

SoD is both an IT "best practice" and an audit and control standard that reduces the risk of a malicious or inadvertent breach of system security, data integrity, or the disruption of normal business processes, by requiring that individuals or workgroups not be in a position to control all parts of a transaction or business process. In finance, responsibilities are divided between different people to assure a single person does not perform every aspect of a financial transaction. Segregating responsibilities can reduce errors and prevent or detect inappropriate transactions.

SoD requires segregating functions by assigning roles and limiting access to individuals based on their job roles. This prohibits one person from giving an account unauthorized access levels (e.g., the authority to change pay rates, update grades, view confidential data, etc.), modifying the underlying system security (i.e., modifying a user's roles, disabling audit functions, etc.), and reviewing system logs or audit reports which could alert an independent reviewer of potential system misuse[7].

A role is a grouping of application permissions assigned to people sharing the same job. Role-based provisioning provides user access to data and applications based on their job function or role. If roles and responsibilities are not followed, the opportunity for collusion cannot be controlled within an organization's risk preferences or within any acceptable framework[8].

University Policy

The University of California policy BFB-IS-3: *Electronic Information Security* (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.

[6] NIST website: https://csrc.nist.gov/glossary/term/separation_of_duty.
[7] AICPA website: https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html.
[8] ISACA website: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/implementing-segregation-of-duties-a-practical-experience-based-on-best-practices.

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

UCSB Guidelines for Financial Management[9]

Accountability for financial control purposes is the delegation of authority to qualified persons to initiate, approve, process, and review business transactions and the holding of those persons responsible for the validity, correctness, and appropriateness of their actions.

A person who delegates tasks must keep a secure, up-to-date record of those delegations as well as modifications to them. A Department Security Administrator (DSA) should be designated to maintain this record.

Department Security Administrator

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

- Provide appropriate access for all on-line preparers and the prescribed PAN 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.

SCOPE AND METHODOLOGY

The scope of our review was limited to identifying critical systems on campus and documenting how roles are assigned to guarantee appropriate separation of duties. The review was limited to the following five financial applications on campus:

- Cashnet
- Transfer of Expense (TOE)
- Transfer of Funds (TOF)
- Travel (TRVL)
- Form 5 Online/Disbursement (DISB)

[9] BFS website – Controller files or documents on financial management guidelines.

Specifically, we:

- Conducted an interview of DSAs and documented their process of assigning roles to users.
- Obtained logs of current role modifications, and:
    - Requested the documentation covering the modification.
    - Identified DSAs who assigned roles to themselves.
- Verified that all users and DSAs of critical applications are active employees of UCSB.
- Documented the exception process and determined exceptions such as whether the access rights of external contractors/employees are appropriate.
- Selected a sample of critical financial applications on campus, and identified critical, and conflicting roles by interviewing application owners and determined whether roles are assigned based on job roles.
- Obtained transactions for the sampled applications and determined whether any single transaction was submitted and approved by the same user.
- Obtained a report of all users and their roles for the sampled critical systems. Developed a role matrix to identify:
    - Users with incompatible roles
    - Users with administrative roles
    - Users with unnecessary/too many roles
    - Users with access to data based on the need to know
- Identified if there are periodical reports to monitor roles and users and if these reports are distributed to the DSA or departments for:
    - Conflicting roles / administrative roles
    - Submitting and Approval transactions
    - Active user accounts
    - Unusual logins

CRITERIA

Our review 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 review was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.* The following documentation:

- University of California – Policy BFB-IS-3: *Electronic Information Security*
- NIST-SP-800-53Ar4 - *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*
- BFB-BUS-10*: Principles of Accountability with Respect to Financial Transactions*
- UCSB *Guidelines for Financial Management*

AUDIT TEAM

Ashley Andersen, Audit Director
Antonio Mañas-Melendez, Associate Director
Gifty Mensah, Senior Auditor