ctcLink Security Audit

Purpose: Periodic security audits are an essential part of governing user access and implementing the principle of least privilege in ctcLink. Security audits help to confirm that role assignments and authorization levels are correct, to mitigate access risks, and to ensure audit readiness.

Audience: Local Security Administrators (LSAs)

User Access

The security process for new hires and terminations should be managed on an “as needed” basis, as personnel are hired or terminated. Steps should be put in place to ensure that accounts are being offboarded in a timely manner, accounts are being set up with the appropriate access for new hires, and the appropriate authorization has been provided and documented.

Each college may have its own business processes for handling each of these procedures; however, the procedures should be documented and followed. Procedural guidelines for setting up and terminating accounts are outlined below.

New Hires

Work with the Pillar Lead or Supervisor to determine the level of access needed for that individual, gain approvals and save all authorization documentation.

When onboarding a new hire, it is critical to consider any segregation of duties issues while assigning roles. Segregation of duties is an administrative control to prevent fraud, theft misuse of information, or other security compromises.

> See Segregation of Duties Section Below.

Assign roles, configure user preferences settings, and set up secondary security as needed.

Reporting Tools > BI Publisher > Query Report Scheduler. BI publisher report: **BFS_SEC_OPDF**

The User Preference Report is located at

> Set Up Financials/Supply Chain > Common Definitions >User Preferences > User Preferences Report.

It can be run for an individual user or for all users.

When establishing a new user in the Campus Solutions pillar, four pages within SACR Security must also be established for each user (at a minimum) to grant access to the data for the college in Student Records. The SACR Security pages listed below must have user access defined in order, as the access builds upon the prior page having been established. Depending on the 'Z' roles granted to the user, (for example ZZ CS Test Score), additional SACR Security may be needed to grant access to specific information or provide the capability to perform certain actions.

CS 9.2 SACR Security: Basic Requirements for Staff

Terminated Users

Upon notification of terminations, the local security administrator should run the QHC_SEC_HR_STATUS_SYSTEM_LEVEL query in HCM to see if the user is active at another institution. If they are active at another institution, the LSA must coordinate with the LSA contact at the other institution prior to offboarding security access. If the user is fully inactive in the system, then the LSA should remove all elevated roles except those listed in the offboarding procedure below. Terminations should be reviewed often to confirm that terminated user accounts are cleaned up with roles removed. All secondary security must be offboarded as well. This is outlined in the 9.2 Offboarding Security Procedure below.

9.2 Offboarding - Security Procedure

To run the terminated user query, follow the navigation: Reporting Tools > Query > Query Viewer:

QHC_HR_SEPARATED_EES_BY_DT

To view the status (and college locations) of an individual user profile, run the query:

QHC_SEC_HR_STATUS_SYSTEM_LEVEL

To interpret this query's results see QRG: 9.2 Employee HR Status System:

https://ctclinkreferencecenter.ctclink.us/m/79718/l/1514278-9-2-employee-hr-status-system-wide

To see which roles the user has assigned that are NOT on the local role grant list, run the query:

QXX_SEC_USER_ROLES_NOT_LOCAL (QXX denotes the pillar, i.e. QCS-CS, QHC-HR, and QFS-FS)

Open a service ticket to request removal of roles not on the local role grant list by the ctcLink Security Team.

9.2 SACR Security - User Replacement Security (Onboarding/Offboarding)

Current Users

When a user’s job function changes, the security administrator will need to update the user’s security request form, get authorization from the user’s manager, and change his or her access within the PeopleSoft Financials system. ctcLink.

Security administrators are responsible for unlocking resetting user accounts and resetting passwords if they expire.as needed.

Documentation and Approvals

Whether your institution requires a printed copy of a security request form or has an electronic system to track security requests and approvals, you must periodically review the requests and recertify users. The main message here is that you cannot have a verbal request for security access with no backup documentation. It must have a signature or electronic approval that can be audited.

Monitoring

It is recommended that user access be reviewed at least once twice a year. Review all user accounts for:

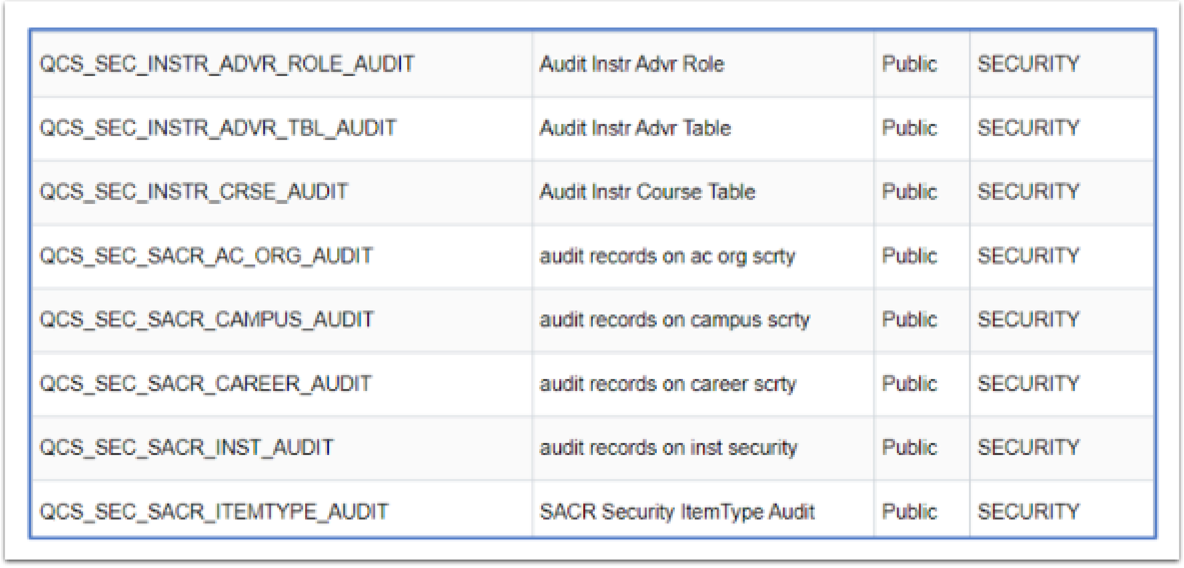
- Level of access (too much or not enough)

- Type of access (have they changed job functions)

- Need of access (do they still need access)

Campus Solutions

- QCS_SEC_USER_ROLES_BY_UNIT query
- QCS_SEC_ROLE_NAV_ACCESS_USER helps determine navigations a user has access
- BCS_SEC_SACR BI Publisher
- SACR security
- **QCS_SEC_SACR_ITEMTYPE_OPR_DTL**
- Review roles in relation to college (ZZ SS Students, ZZ SS Faculty, ZZ_CS_Staff & ZZ SS Advisors).
- OAAP (online admissions application) security review.



QCS_SEC_INSTR_ADVR_ROLE_AUDIT	Audit Instr Advr Role	Public	SECURITY
QCS_SEC_INSTR_ADVR_TBL_AUDIT	Audit Instr Advr Table	Public	SECURITY
QCS_SEC_INSTR_CRSE_AUDIT	Audit Instr Course Table	Public	SECURITY
QCS_SEC_SACR_AC_ORG_AUDIT	audit records on ac org scrty	Public	SECURITY
QCS_SEC_SACR_CAMPUS_AUDIT	audit records on campus scrty	Public	SECURITY
QCS_SEC_SACR_CAREER_AUDIT	audit records on career scrty	Public	SECURITY
QCS_SEC_SACR_INST_AUDIT	audit records on inst security	Public	SECURITY
QCS_SEC_SACR_ITEMTYPE_AUDIT	SACR Security ItemType Audit	Public	SECURITY

Human Capital Management

- QHC_SEC_USER_ROLES_BY_UNIT
- QHC_SEC_ROLE_NAV_ACCESS_USER helps determine navigations a user has access
- CTC_EE_SUPER_LIST
- ZZ LegacyLink & ZZ Legacy Transcripts access audit

Finance

- QFS_SEC_USER_ROLES_BY_UNIT
- QFS_SEC_ROLE_NAV_ACCESS_USER helps determine navigations a user has access
- BFS_SEC_OPDF_BI Publisher
- Secondary User Preferences security

> The person who reviews the security request forms should maintain signed documentation that the user accounts were reviewed. These forms should be stored on top of the security request form on file for audit purposes or stored electronically and should include items such as segregation of duties review, user preferences review, and budget security reviews.

Segregation of Duties

It is critical to review Segregation of duties issues twice a year for audit purposes. Run the queries:

QFS_SEC_SEGREGATION_OF_DUTIES

QHC_SEC_SEGREGATION_OF_DUTIES

QCS_SEC_SEGREGATION_OF_DUTIES

These queries are based on a Segregation of Duties (SOD) which identifies Process/Functions and role names that may be considered a segregation of duties issue.

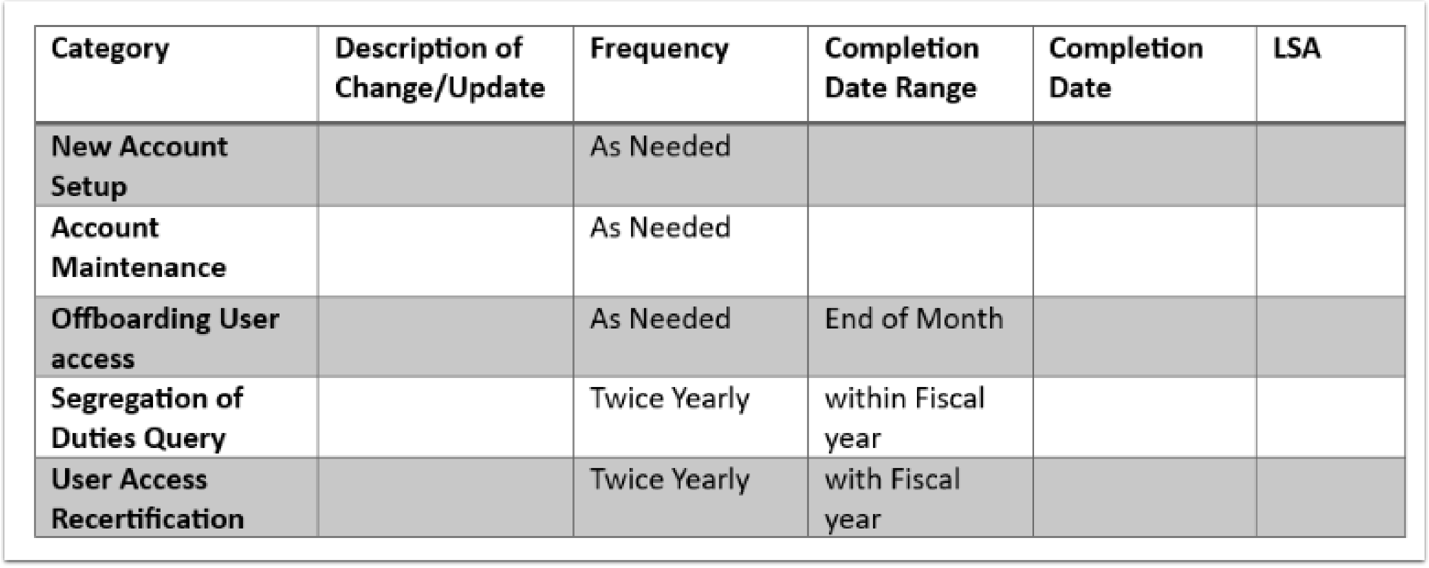
If a user appears on this query, it does not necessarily mean that they are in violation. However, the college security administrator should do further research to ensure that the user's access is not a violation and should then annotate the research for the auditors. If it is a violation, the security administrators should work with the Business Office to determine what access to remove from the user. If the college is a smaller college and access cannot be removed due to resource issues, mitigating controls must be put into place. The controls have to be documented, approved and followed, and the institutions will have to prove the procedure is followed.

Audit Checklist

It is recommended that a binder be established, and a copy of this checklist placed on the front for reference by the auditors. Complete each item as needed and record the actual date of completion. There are several categories, and within each category, there may be several tasks. These tasks will be listed out in procedures that will be distributed as part of this packet. For example, within account maintenance, there may be changes in a user's job function that would require the security administrator to make a security change in the system, as well as get an updated and signed security request form. Password resets and lockouts would also fall under the account maintenance category.

Not only does an institution need to keep a copy of the checklist, but it is recommended that all associated policies and procedures that correspond to the checklist be kept together. Any documentation associated with a change that is made in the system should be kept together so that it can be handed directly to the audit staff. Keep all security request forms, changes, updates, and annual review forms to ensure compliance.

Audit Checklist



Category	Description of Change/Update	Frequency	Completion Date Range	Completion Date	LSA
New Account Setup		As Needed			
Account Maintenance		As Needed			
Offboarding User access		As Needed	End of Month		
Segregation of Duties Query		Twice Yearly	within Fiscal year		
User Access Recertification		Twice Yearly	with Fiscal year		

Example Security Audit topics:

Auditors review applicable laws, rules, business procedures; interview personnel; and examine records to obtain an understanding of operations related to PeopleSoft Applications and to evaluate whether business operations are designed properly and operating effectively.

Evaluate and test key processes, procedures, and controls related to the IT processes for PeopleSoft Applications infrastructure, including authentication, logical controls, vulnerability management, logging and monitoring of the network, application, and database servers (servers), and the database management systems (databases), and PeopleSoft modules, supporting server, database, and network device change management.and authorization.

Evaluate the effectiveness of logical access controls assigned to the network, servers, and databases supporting PeopleSoft Applications, including the periodic evaluation of assigned accounts.

Evaluate the effectiveness of logical controls assigned within the PeopleSoft modules, including procedures related to the periodic evaluation of assigned user access privileges.

Evaluate selected security settings related to PeopleSoft Applications and the supporting infrastructure to determine whether authentication controls are configured and enforced in accordance with IT best practices.

Evaluate procedures and examine selected scan reports and policies to evaluate the adequacy of vulnerability management controls related to the PeopleSoft Applications supporting IT infrastructure, including vulnerability assessment and remediation, maintenance, monitoring, and analysis of audit logs and malware defense.

Examine and evaluate the appropriateness of all accounts assigned administrator access privileges.

Examine and evaluate the appropriateness of access privileges granted on the servers supporting PeopleSoft Applications.

Evaluate procedures related to the recording, documenting, and reporting of changes to confidential and critical student record information within PeopleSoft Applications Campus Solutions to determine the adequacy of logging and monitoring controls related to student information.

Examine and evaluate the appropriateness of access with access identification allowing the ability to modify historical grades.

Evaluate procedures and selected records related to PeopleSoft Application upgrades and changes to determine whether modifications required appropriate authorization, testing, and approval.