CAPITAL PROGRAMS

CapSTAR SYSTEM REVIEW

AUDIT REPORT #17-2001

Audit & Advisory Services

January 2017

CAPITAL PROGRAMS

CapSTAR SYSTEM REVIEW

AUDIT REPORT #17-2001

Background

In accordance with the Campus fiscal year 2016-17 audit plan, Audit & Advisory Services (A&AS) conducted an audit of internal controls and associated procedures established to operate and safeguard Capital Program’s Capital Projects Status, Tracking, and Reporting (CapSTAR) system and its underlying data.

CapSTAR is a proprietary software system that was originally designed by the Capital Programs Information Systems (IS) unit in 1989. The system was developed to integrate data from the multiple functions of capital project management to enhance the effectiveness of project managers and Capital Programs’ senior management. Through a centralized dashboard, users have access to a database that contains information related to their projects. The system is designed with eight modules, including contract management, project management, accounting, personnel time entry, and other essential capital project-related functions.

The first version of the application was deployed in 1990s. Since then, multiple system upgrades have been performed by Capital Programs IS personnel with the assistance of independent consultants. The web-based application allows CapSTAR users to access the application remotely through a web browser. The IS unit adopted an “iterative” development process, with enhancements that are added to the application continuously, based on users’ feedback.

The system is widely used by Capital Programs personnel and other capital project development personnel across the University, including users in Housing & Hospitality Services, Facilities Management, and UCLA Health.

The IS unit is overseen by the Network/Software Manager who reports to the Director of Administrative Services. Two network administrators and a database administrator report to the Network/Software Manager. The unit is responsible for CapSTAR and other Capital Programs-specific applications. Responsibilities also include supporting CapNet, the Capital Programs local area network; the basic business software applications; certain specialized project design and management software applications supplied by outside software vendors; and acquisition and support of central network and end-user hardware.

Purpose and Scope

The primary purpose of the review was to ensure that Capital Programs organizational structure and controls surrounding the operation and maintenance of CapSTAR are conducive to accomplishing its business objectives. Where applicable, compliance with campus and University requirements was also evaluated.

The scope of the audit focused on the following areas:

* User Access Administration
* Physical Controls
* Cyber Security Awareness and Password Security
* Business Continuity and Disaster Recovery

The review was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* and included such tests of records, interviews, and other auditing procedures considered necessary in achieving the audit purpose.

Summary Opinion

Based on the results of the work performed within the scope of the audit, the Capital Programs organizational structure and controls surrounding the CapSTAR system are generally adequate and effective to help achieve its business objectives. However, the following business practices could be further strengthened to improve upon the existing internal controls:

***User Access Administration***

* A review of CapSTAR users should be performed at least annually to ensure that only active University employees have access to the system. Access to CapSTAR should be removed within a timely manner when an employee separates from the university or is placed on an inactive status. Access should be temporarily disabled whenever an employee is placed on a leave of absence.
* A three-phase approach could be implemented to administer user access for internal users of CapSTAR. The approach would start from a minimum of timesheet access, to functional roles access, and finally to specialized access, as needed. The assignment of user access should also be documented for oversight and accountability purposes.

***Physical Controls***

* Server racks should be properly secured to reduce the risk of damage to equipment during seismic activity and to prevent personal injury.

***Cyber Security Awareness and Password Security***

* Management should ensure that all Capital Programs staff complete the Cyber Security Awareness training in a timely manner.
* Password requirements to access the CapSTAR system and its server should meet the minimum complexity standards outlined by the university.

The audit results and corresponding recommendations are detailed in the following sections of the report.

Audit Results and Recommendations

User Access Administration

The CapSTAR system has two types of users – internal and external. Internal users include all of Capital Programs management and staff. External users are employed by the University, but are not part of the Capital Programs department. External users include management and staff from Facilities Management, Housing & Hospitality Services and UCLA Health.

Two separate electronic listings showing the 172 CapSTAR users and their access type were obtained from Capital Programs IS staff on August 1, 2016. A&AS utilized data analytics (e.g., queries, pivot tables, filters, sorts, etc.) to compare information from the entire population of users against the University’s Employee Database (EDB) to identify each user’s access type and employment status. Based on this user listing, controls over the administration of CapSTAR accounts were reviewed to ensure that access is restricted to active employees, and that sensitive data and records are limited to authorized personnel. A judgmental sample of 42 active CapSTAR users (32 internal and 10 external) was also selected for review to verify that users’ role assignments and permissions were appropriately approved.

Test work performed included inspection of relevant documentation, review of established procedures and discussions with staff regarding assigning access rights and permission practices. The following were noted:

1. Access Controls

Based on the test work described, access to CapSTAR sensitive data (i.e., personnel-related information) and records is limited to the department’s Personnel Manager and other authorized staff. For the sample of external CapSTAR users selected, A&AS determined that functional role permissions assigned were appropriately approved. Specifically, external CapSTAR users are required to submit an online access request form through the department’s website. Online access request forms are submitted to IS unit staff for review and approval. However, our review also noted the following:

* Six individuals were identified as having access to the CapSTAR system even though they were not current active employees. Specifically, four of the six individuals had separated from the University; one employee was on inactive status; and one employee’s access had not been deactivated while out on a leave of absence since April 2016. A&AS noted that one of the four separated employees was a post-retirement, part-time rehire to the department. Capital Programs staff indicated that rehire paperwork was prepared concurrent with the employee’s retirement. In addition, since the separation was treated as an extended leave of absence, the 34-day gap between separation date and rehire date was not thought to be an issue for maintaining the employee’s access to CapSTAR.
* Although access to CapSTAR from internal users appears appropriate, current business practices for the administration of role assignments could be strengthened. Capital Programs formerly granted internal user access to CapSTAR based on the completion of a “Request Access Form.” This practice was discontinued several years ago and replaced with an online request form. Based on the department’s current business practices, newly-hired Capital Programs employees are typically granted identical access as their predecessor or access is copied between staff within the same functional unit (e.g., Finance, Project Management, etc.). Any additional or specialized CapSTAR access is provided by IS staff upon request or as needed. As a result of the existing practice, there is a risk that an individual could inadvertently be assigned an inappropriate level of access based on what was granted to their predecessor.

Recommendation: To strengthen controls over access controls, management should:

* Perform a periodic review, at least annually, of CapSTAR users to ensure that only active University employees have access to the system. Users who are identified as separated or inactive should have their access terminated on a timely basis. Employees who are on a leave of absence should have their CapSTAR access temporary disabled. To assist in improving this business practice, A&AS can share the query used to perform data analytics comparing the population of users against EDB information.
* Based on best business practices, the Capital Programs IS unit could implement a three-phase approach to administering access for internal users of CapSTAR. This approach would grant access in three phases starting from a minimum of timesheet access, to functional roles access, and then finally to specialized access, as needed. The three-phase approach could help ensure that staff is provided appropriate level of access to the CapSTAR system on a timely basis. Capital Programs IS staff should collaborate with each internal department unit to determine appropriate access for each functional role. The assignment of user access should also be documented for oversight and accountability purposes.

Response: IT staff currently performs an annual review of external CapSTAR users (still UCLA employees). We email a department representative with a list of that department’s CapSTAR users and request that the representative confirm the user’s continuing need to access CapSTAR. In addition, we deactivate accounts with no activity for 60 days.

To create a more timely deactivation of an external CapSTAR user account, IT staff will work on a new mechanism to determine active UCLA Employees.

Although IT staff currently has a formal checklist procedure for new hires and departing users, IT staff will work on a new work flow procedure for Internal Users where a department manager / Supervisor will have to specify the specific rights to be assigned to the new employee. And any verbal communications with managers will be replaced by a more documented process.

1. Super User Review

Controls surrounding Super User activity (i.e., administrator role access) were tested to determine whether administrator activity is logged and reviewed. Based on discussions with IS staff and review of relevant documentation, A&AS determined that Super User activity is tracked on an audit log and a user access log. The audit log tracks all changes made to a particular record within the system’s database. Due to the high volume of records within CapSTAR, system audit logs are only reviewed upon Capital Programs management request or special circumstances. The user access log is a continuous listing that tracks a user’s activity within the application by time and date. For instance, the user access log documents when a module or document was accessed by an individual. Data provided by the user access log is compiled by IS staff and provided to Capital Programs management for review, upon request.

There were no significant control weaknesses noted in this area.

Physical Security

A&AS reviewed controls over the Capital Programs server room to verify whether the CapSTAR web and database servers are properly safeguarded, and the room is adequately protected against intrusion. Observations and discussions were conducted with Information System staff to evaluate whether the desired environmental factors for the server room are adequately maintained. The following was noted:

1. Physical Security

On September 20, 2016, A&AS performed a physical security walkthrough of the Capital Programs server room. Based on discussions with management, it was noted that access to the server room is restricted to IS staff and the building’s operations manager. The server room is secured during and after business hours.

During the observation, A&AS determined that the Capital Programs server room is adequately ventilated through the building’s central air conditioning system. A back-up air conditioning system is installed within the server room to prevent excessive heat accumulation in the event that the building central cooling system malfunctions or fails altogether. The server room is monitored by a smoke detector/alarm and is equipped with a Class B and C rated fire extinguisher for liquids and electrical equipment. Servers, network attached storage (NAS) devices, uninterruptible power supply (UPS) devices, and other equipment are maintained on six server racks located throughout the room. Each server rack is supplied power by the building. A UPS device is installed at each server rack to provide 5 minutes of continuous power in the event of a power outage. A&AS identified the following:

* Four of the six server racks have seismic bracing installed to prevent movement and injury during seismic activity or an emergency. However, two of the four server racks are not properly secured to the building. Additionally, there is no evidence that the remaining two server racks have seismic bracing installed or are properly secured.
* The Capital Programs server room is equipped with a water-based fire sprinkler system. Since electrical equipment is maintained within the server room, there is a risk of potential water damage to the department’s information technology infrastructure if the sprinklers are activated or malfunction. The risk of water damage will continue to exist as long as the sprinkler system is in use as a fire suppression system. Capital Programs management has obtained a quote and is currently considering a clean agent (non-water based) fire suppression system for the server room.

Recommendation: Management should ensure that server racks have seismic bracing installed and that they are properly secured to help prevent the risk of movement and/or injury during an emergency. Management should also continue its evaluation and consideration of the feasibility of a clean agent fire suppression system for the server room to help mitigate the risk of loss.

Response: IT staff will work to ensure that the server racks have appropriate seismic bracing. IT staff will continue to work with management on an appropriate solution to the water sprinkler problem in the server room.

Cyber Security Awareness & Password Security

On October 22, 2015, the UCLA Office of Executive Vice Chancellor notified the campus of the new requirement that all employees on active payroll status must complete Cyber Security Awareness Training by January 31, 2016. New hires after January 31, 2016, had six weeks to complete the training to be in compliance with the mandate. A&AS evaluated the extent to which Capital Programs personnel were in compliance with the new UC Systemwide training requirement. Controls over passwords were also reviewed for adequacy and to determine whether users have been trained on the proper handling of user IDs and passwords. Password storage practices were reviewed to determine that they are maintained in such a way that precludes viewing by system administrators. Capital Programs’ password complexity practices were also reviewed for compliance with University policies. Discussions were conducted with IS staff and relevant documentation was reviewed. The following were noted:

1. Cyber Security Awareness

Based on discussions with the University’s Learning Management System personnel and review of relevant documentation, the majority of Capital Programs management and staff had completed the Cyber Security Awareness Training by the prescribed deadline. However, A&AS identified six Capital Programs employees that had not completed the training, as of the date of our review (August 15, 2016). All six of the employees identified were on payroll and had an active status shown in EDB. None of these employees were recent hires.

Recommendation: Management should ensure that all Capital Programs staff complete the required Cyber Security Awareness Training as soon as possible. Going forward, the Cyber Security training should be completed by all department employees on an annual basis or within six weeks of a newly-hired employee’s start date.

Response: IT staff will coordinate with the Capital Programs HR Manager to confirm compliance.

1. Password Security

Discussions with Capital Programs IS staff and a review of relevant documentation disclosed that CapSTAR users are notified in writing of the importance of not sharing their logon ID and password. Users are required to change their default password when they initially log into their account. Passwords are masked within the CapSTAR system to preclude administrators or others from viewing them. User IDs and passwords are also encrypted within the system’s database to maintain their integrity. A&AS noted, however, that password complexity standards for the CapSTAR system and its server do not meet the minimum security standards outlined in UCLA Policy 401, Minimum Security Standards for Network Devices, Attachment A. Current Capital Programs practice instructs new CapSTAR users to choose a password with a minimum of seven characters, preferably with a combination of letters and numbers.

Campus policy requires a more stringent standard for setting passwords. UCLA Policy 401, Attachment A states the password must contain eight characters or more, including characters from at least two of the following three character classes:

* Letters (a-z, A-Z)
* Numbers (0-9)
* Special characters including a space (: !@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)

Capital Programs IS personnel indicated that there are no inherent system constraints that would preclude adherence to the above campus policy.

Recommendation: Management should ensure that the department’s password practices comply with the requirements set forth in UCLA Policy 401. Existing practices should be reexamined and revised to better align with campus standards.

Response: IT staff is currently working on a new version of CapSTAR and will work with Management to establish new password requirements that comply with the minimum standards set forth in UCLA Policy 401.

Business Continuity Plan and Disaster Recovery

A&AS conducted meetings with Capital Programs staff, communicated with UCLA Insurance and Risk Management, and reviewed documentation related to business continuity and disaster recovery planning for department operations and, in particular, the CapSTAR system. Audit procedures were performed to determine whether business continuity and disaster recovery planning was current and adequately documented for the CapSTAR system. Based on our review, Capital Programs has established a business continuity plan, including documentation relating to the CapSTAR system, on the UC Ready database. UC Ready is a systemwide tool designed to assist campuses in developing their business continuity plans. A disaster recovery plan has also been created for CapSTAR to supplement the system’s business continuity plan.

The disaster recovery plan provides specific actions, responsible parties, and time frames when responding to various emergency situations. To help ensure that Capital Programs and external departments that use CapSTAR (Facilities Management, Housing & Hospital Services, and UCLA Health) can continue business operations, a CapSTAR back-up website operates from an off-site location to provide access to the University’s critical information in the event of an emergency. Capital Programs and UCLA’s Insurance and Risk Management units are actively collaborating to ensure that the department’s business continuity and disaster recovery plans are maintained and available within the UC Ready database.

There were no significant control weaknesses noted in this area.

161122-2