CAPITAL PROGRAMS

SHAREPOINT SYSTEM REVIEW

AUDIT REPORT #18-2103

Audit & Advisory Services

June 2018

CAPITAL PROGRAMS

SHAREPOINT SYSTEM REVIEW

AUDIT REPORT #18-2103

# Background

In accordance with the Campus fiscal year 2017-18 audit plan, Audit & Advisory Services (A&AS) conducted an audit of internal controls and associated business practices established to administer and safeguard the UCLA Capital Programs SharePoint system (SharePoint) and its underlying data.

Capital Programs Overview

The Capital Programs department is responsible for conceptualizing, planning, designing, and constructing major capital construction and renovation projects at UCLA. Projects having total costs of $750,000 and above are considered major capital construction. Since its establishment in 1986, Capital Programs has expended approximately $6.1 billion to complete a variety of new construction, renovation, and infrastructure projects; two replacement hospitals and related parking facilities; nearly 55 new buildings or building complexes; 27 major building additions; and five new parking facilities. In addition, seismic renovations have been completed on approximately 60 buildings, and a large number of existing buildings throughout the campus have been modernized. Capital Programs develops financial strategies, obtains project approvals, reviews plans and specifications, completes environmental reviews, prepares and negotiates construction contracts, coordinates staging plans, and serves as a repository for project records and as-built plans.

The department’s mission is to create projects that “support the instruction and research mission of the University by providing a physical campus environment that fosters excellence, creativity, and a sense of community.” Capital projects are developed to take into account UCLA land use priorities, established physical designs, University policies and procedures, environmental and regulatory requirements, and community interests.

Capital Programs consists of two organizational units:

*Capital Planning and Finance* – responsible for planning, environmental assessment, project budgeting, information technology, personnel, and project financial services including contracts administration. This area is led by an Associate Vice Chancellor who reports to the Vice Chancellor and Chief Financial Officer.

*Design and Construction* – responsible for project design, project management, and construction management. This area is headed by an Associate Vice Chancellor who reports to the Vice Chancellor and Chief Financial Officer.

SharePoint Overview

Microsoft’s SharePoint is a web-based document management system that Capital Programs deployed for use in December 2010. The software was upgraded to the 2013 Enterprise Edition in December 2016, which improved the performance of the system. The application is integrated with the Microsoft Office suite, and allows Capital Programs the ability to better organize, manage, share, and secure documents. Prior to SharePoint, documents were stored on network drives and shared via e-mail or in hardcopy format, a system which lacked the level of organization and control that department management desired. With SharePoint, project or unit specific websites are created to house documents and provide a platform for collaboration, which can be accessed and shared from multiple devices at any location. Document versions can be controlled and managed, and access rights can be assigned to a particular folder level. SharePoint is installed on the Capital Programs department servers, and is administered by its Information Technology (IT) unit.

# Purpose and Scope

The primary purpose of the audit was to evaluate manual and automated controls, procedures, and security protocols. Where applicable, compliance with campus and University policies and procedures were also evaluated.

The scope of the audit focused on the following areas:

User Access Administration

Audit Logs

Backup and Recovery

Business Continuity and Disaster Recovery

The review was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing* and included interviews, tests, and other procedures considered necessary to achieve the objective.

# Summary Opinion

Based on the results of the work performed within the scope of the audit, internal controls, including the related procedures and security protocols over the administration of SharePoint, were generally conducive to accomplishing its business objectives. However, controls and business practices could be further strengthened by implementing the following:

SharePoint external user access requests should be approved by the appropriate project manager (or supervisor) prior to granting access to the system.

* Develop a procedure or workflow to identify external users in a timely manner who have separated from the University or have transferred departments.
* Develop policies and procedures to administer log management activities for the SharePoint system.
* Complete the department’s internal review and update of the Capital Programs Business Continuity Plan.
* Develop a protocol for periodically testing and documenting backups of SharePoint data.

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

# Audit Results and Recommendations

## User Access Administration

The SharePoint system has two types of users – internal and external. Internal users include all of the Capital Programs management and staff. External users include those individuals employed by the University, but are not part of the Capital Programs department (e.g., Facilities Management, Housing & Hospitality Services, UCLA Health, Information Technology Services, and A&AS). The external users group also includes two outside consultants.

SharePoint allows an organization to assign the same permission level to many people concurrently through the use of user groups. A user group is defined as a collection of individuals who use a SharePoint site in similar ways and require the same permission level. At the time of the audit, the department had created 21 user groups, loosely based on Capital Programs operational units and other University departments. Although the SharePoint application offers several standard levels of access, Capital Programs currently uses just five permission levels (see Table 1).

**Table 1**

|  |
| --- |
| **Capital Programs SharePoint Permission Levels** |
| **Permission Level** | **Description** |
| Full Control | Has full control |
| Contribute | Can view, add, update, and delete list items and documents |
| Limited Contribute | Can view, add, and update list items and documents |
| Read | Can view pages and list items and download documents |
| View Only | Can view pages, list items, and documents. Documents can be viewed in the browser but not downloaded. |

A SharePoint site connects team members to the content, information, and applications. When providing access, each user is added to the particular site collection or to specific folders. Of the numerous SharePoint sites available, Capital Programs currently uses two main categories:

1. Departmental Unit Sites: These sites contain shared calendars and documents that are used in a collaborative manner. Internal users within this department unit SharePoint site have “Contribute” rights. Internal users not in this department unit only have “Limited Contribute” rights.
2. Project Sites: These sites have shared calendars and documents related to specific projects. Internal users have “Contribute” rights, and external users are assigned “Limited Contribute” rights.

Interviews were conducted with IT unit staff to obtain an overview of departmental processes, procedures, and controls over access to SharePoint system.

### Internal User Access Controls

A review of the applicable workflows and discussions with management were conducted to determine whether the process used to grant access to SharePoint for new Capital Programs employees is adequate and that user privileges can be associated with particular job roles and responsibilities.

Capital Programs currently utilizes Document Management workflows to initiate the account creation process for internal users and to coordinate tasks that are part of the new hire process. Document Management is a Capital Programs application that was developed to share and collaborate on various documents. After the Personnel Manager creates a workflow, the new employee's supervisor approves the instructions in the workflow. The supervisor communicates to the IT unit the type of user rights to be assigned and provides the name of an existing employee that has a similar job role to the new employee. The Database Administrator then creates a user account from the Active Directory, and the Network Administrator adds the account to the SharePoint system and sets up the user rights for the new employee. The workflow process concludes after an initial training is provided to introduce the new employee to the department systems.

There were no significant control weaknesses noted in this area.

### External User Access – Approvals

External users from organizations with delegated authority to manage selected construction projects (such as Facilities Management, Housing & Hospitality Services, and UCLA Health) can be granted access to specific folders within SharePoint sites to facilitate the project design, project management, and construction management processes. Before requesting access, external users must first complete the Capital Programs Single Sign-on registration form to apply for a user account. After agreeing to department policy and guidelines, and submitting the form, the applicant is sent a link to verify their e-mail address. Once an account is created, users can then request access to SharePoint by completing the online SharePoint Request Access form. A notification is sent to the relevant Project Manager who was noted on the request form. Access to applicable SharePoint sites and folders is typically granted within 24 hours.

Internal controls surrounding the process for creating external user accounts were reviewed and discussed with department management. An electronic listing showing the 225 SharePoint users, designated groups, and their access to site collections, was obtained from Capital Programs IT personnel on October 17, 2017. A judgmental sample of 15 external users from the above delegated departments were selected for audit testing and to verify whether a SharePoint Request Access form was properly completed, and that access was authorized by a Project Manager (or supervisor) prior to granting system access.

Based on the test work performed, A&AS noted that 13 of 15 users (87%) in our sample did not complete the request form. Management explained that one user account was created in February 2014, before the access forms were in effect; however, the other 12 user accounts tested were created during a transition period in 2017. According to IT unit staff, the number of new SharePoint users increased by 100 to 150 employees between March and May of 2017, due to the roll out of the new version of SharePoint (v. 2013) to the delegated entities. Staff at those entities could begin utilizing their access to review and approve contract documents for their projects.

To temporarily streamline the approval process, Capital Programs personnel generated a list of new and existing users to enable management from the delegated entities to review and confirm. This temporary process was used in place of requiring each user to complete an online application. After the initial wave of new user accounts were created for the delegated entities, Capital Programs returned to utilizing its standard practice of requiring completion of the online SharePoint Request Access form for each new user account.

Audit testing of external user access also noted the following:

An individual was inadvertently granted access to the SharePoint system four and a half years after the employee had separated from the University. The access was subsequently removed four to five months after the user account was created. Management stated that the account creation was initiated by Capital Programs during the period when lists of delegated users were sent to management of those departments for review and confirmation of ongoing active status. This individual was apparently not flagged for removal by the delegated department and, therefore, was not deactivated by Capital Programs IT personnel.

Project Managers from the delegated departments are notified via e-mail when employees under their supervision request access to SharePoint. However, Capital Programs IT staff does not require Project Managers to confirm and approve their subordinate SharePoint applicants before access is provided. With the current practice, an individual could potentially gain unauthorized access to certain sections of SharePoint information if the appropriate manager does not promptly confirm the access request. Capital Programs IT staff indicated that if an individual were to temporarily gain unauthorized access, the user would not be able to delete any files but could view and update information in a limited number of folders within SharePoint.

Recommendation: Management should consider requiring that external user access requests to SharePoint are first approved by the appropriate project managers (or supervisors) prior to granting access to the system.

Response: IT staff has implemented a work flow process to incorporate a step for remote Managers to approve the SharePoint request.

### External User Access – Appropriateness

The employment status, site permission levels for each group, and a list reflecting the site collections assigned to each user were reviewed to verify that the access of the 15 selected users is appropriate. The sample users tested were all granted “Limited Contribute” rights to the proper site collections based on the departments where they are employed. However, A&AS noted that there is a delay in terminating SharePoint access for University employees who have transferred departments or have separated from the University. The following were noted:

At the time of the audit, SharePoint system access had not been terminated for two employees who had been separated from the University for 62 and 133 days respectively.

User access was terminated 19 months after a separated employee transferred departments.

As described above, system access was removed four to five months after a user account was inadvertently created for a separated employee.

In total, four of 15 users (27%) appear to have had inappropriate SharePoint access for the time periods noted above. An effective process to monitor user access, and terminate access when appropriate, is an important internal control to help minimize the risk of improper use of information.

Recommendation: Management should develop a procedure to promptly identify external users who have transferred departments or no longer work for the University. This would help to strengthen existing internal controls and ensure that only authorized users are accessing the system.

Response: Management agrees with the recommendation. Currently, there are no automated services available to IT staff, at our security level, from the main campus where daily checks can be made for the change in status of an employee in another department.

### User Review

Capital Programs IT unit personnel were interviewed to gain an understanding of the annual user access review process for the SharePoint system. Correspondence between Capital Programs and management from various campus departments was also examined to verify that the annual review was being conducted, working as designed, and adequately documented.

During discussions with IT unit staff, it was noted that access is not reviewed annually for internal department users. Management explained that access is evaluated when employees separate from Capital Programs or if there are changes in job responsibilities or position. An annual review of access rights for external user groups was conducted and adequately documented, with the exception of two outside consultants. It was stated, however, that the department’s Network/Software Manager communicates with the consultants on a weekly basis and, therefore, an annual access review was determined not to be necessary. During the course of the audit, management indicated that the annual review for external user groups was replaced in October 2017 by a monthly e-mail validation process. The new process, which is still in development, consists of verifying all external user e-mail addresses with the online University directory.

There were no significant control weaknesses noted in this area.

## Audit Log

A&AS reviewed audit log controls to verify that information that allows for tracing of SharePoint activities is maintained. The audit log feature is not enabled in the SharePoint system. The IT unit mentioned that enabling the audit logs will affect the performance of the system. The following activities, however, can be traced using the current compensating controls:

Lists of items that are currently checked-out or have been checked back-in can be accessed. Management indicated that obtaining historical data of checked-out documents would require the IT unit staff to write a computer program to identify and extract this type of information.

The history of modifications made to a specific file can be viewed with the version control feature. According to management, obtaining a comprehensive report showing all items modified by users during a specific period of time would also require new computer programming.

Deleted items can be viewed in the Site Collection (second-stage) recycle bin by an administrator. Management explained that the recycle bins do not have a storage size limit. The total tracking period can vary between 30 to 60 days, depending on the date files were deleted from the site (first-stage) recycle bin.

SharePoint versioning in combination with the check-out and check-in feature is a valuable control that locks documents when they are being worked on and maintains an audit trail of the 20 most recent versions. A new version is created after a modified document is checked-in, and the oldest version is permanently deleted when the limit is reached. Accordingly, the version history could last a few days to several years, depending on how often a document is modified.

A&AS found the following audit trail limitation:

Modifications to SharePoint settings or user rights can only be made by administrator accounts, but the current controls do not allow this type of activity to be tracked in the system. IT staff indicated that, because they are a small unit, only four individuals have administrator accounts. Moreover, having multiple administrator accounts is necessary to facilitate routine maintenance assigned to staff and for back up purposes.

Based on a review of IT resources provided through the UC Office of the President website, one document “Log Management for the University of California: Issues and Recommendations,” dated May 1, 2006, noted that application logs should identify what transactions have been performed, at what time, by whom, and on what object. In particular, applications should log operations that modify permissions or access rights. In order to facilitate investigation as well as to protect privacy, the retention of log records should be well-defined.

Although the existing compensating controls record various events occurring within SharePoint, comprehensive audit logs could provide an additional layer of information that may be beneficial for identifying potential security incidents, policy violations, and operational issues.

Recommendation: Management should develop department policies and procedures for log management that include the SharePoint system. Policies should clearly define log management activities such as log generation, storage, analysis, and disposal. The cost of storage and processing, as well as the potential benefit of having that information at some time in the future, should also be considered when determining which sources should be incorporated into the log management infrastructure. Proper management of audit logs can enhance security, system performance, and resource management.

Response: Management views that the finding of the “Audit Trail” limitation as a non-issue and disagrees with any changes. Individuals with Administrative Rights need that level of access to complete their job duties. SharePoint is a database system, which automatically logs and identifies transactions that have been performed by users, at what time, by whom, and on what files. It maintains a version history of this information based on settings determined by management. Current policy saves the last 20 versions of a document. Rights to delete a file is limited and alerts for the deletion of a file can be setup by any individual. Additional reports or data can be queried from the SharePoint Database as needed.

Administrator login and updates of the server can be viewed through an event viewer of the server logs. The size of the server logs follows the Microsoft Server default settings. In addition, custom queries can be performed on the SharePoint server. These options provide the IT staff with additional analysis of administrator activity, as needed.

## Backup and Recovery

Written procedures regarding backups of computer files were acquired and reviewed, and discussions were held with Capital Programs IT unit personnel to gain insight into the current SharePoint practices. The SharePoint Virtual Machine (VM) is backed up to an on-site storage device on a weekly basis, and at least two copies are retained. Database backups are also created on a daily basis and stored on-site. The SharePoint farm, which serves as the framework for the system, is backed up periodically after SharePoint is updated. In May 2017, the weekly process of uploading the SharePoint VM backup file to an off-site cloud service was implemented. Due to technical issues, the frequency of cloud backups was temporarily reduced from its standard weekly interval. IT unit staff stated that the weekly schedule is expected to resume sometime in January 2018 after a new mechanism for uploading information to the cloud is developed and tested. Overall, the written procedures for SharePoint backups reflect current practices performed by IT unit personnel and those practices appear to adequately protect data from loss.

There were no significant control weaknesses noted in this area.

## Business Continuity and Disaster Recovery

A&AS obtained and examined the Capital Programs business continuity and disaster recovery plans from the UCLA Insurance and Risk Management department to verify that the plans were periodically updated to reflect changing environments, processes, technology, or other impacts as appropriate to the SharePoint system.

### Business Continuity and Disaster Recovery Plans - Updates

Meetings were conducted with Capital Programs staff to determine whether the department periodically reviews and updates their Business Continuity and Disaster Recovery plans, and to walk-through key areas related to the SharePoint system. In a discussion with the Network/Software Manager, A&AS staff were informed that the system restore procedures had not been updated in the current Disaster Recovery Plan due to technical issues that were encountered after the recent implementation of the cloud backup process for SharePoint. The plan will be revised with steps related to the cloud service after a new backup process is developed.

Based on our review, the SharePoint system has been adequately considered within the Capital Programs Business Continuity and Disaster Recovery plans. The plans were last reviewed and updated in July 2017, however, the maximum tolerable downtime of the system documented in the plans do not align with management's expectations. Specifically, the plans indicate a maximum tolerable downtime of less than one day for the SharePoint system, although IT unit personnel indicated that there is no expectation the system would be available within 24 hours. Moreover, a full system restoration from a cloud backup would take at least one to two weeks. Management stated that the Business Continuity plan is not yet finalized. The goal of the department is to review and update the plan during 2018.

Recommendation: A&AS encourages Capital Programs to complete its review and any necessary revisions of the departmental Business Continuity and Disaster Recovery plans that identify critical functions and systems, including information and strategies to recover data and operations.

Response: Capital Programs agrees with the recommendation and is currently reviewing its disaster recovery plans.

### Preparedness

Interviews with key IT unit personnel were held to determine whether the Business Continuity and Disaster Recovery plans were tested on a periodic basis. The SharePoint system was restored from backups on two separate occasions – in December 2016 and January 2017; however, backups are not periodically tested to ensure they will work as designed. IT unit management explained that since the SharePoint system had been previously restored successfully, there is no need to perform recurring tests. According to the UC Policy BFB IS-12 “Continuity Planning and Disaster Recovery,” preparedness is critical to continuity planning and disaster recovery, and plans should be tested on a periodic basis. A “Symantec Disaster Recovery Research 2007” report found that 48 percent of test recoveries run by clients testing their disaster recovery plans failed. Even for simple backups, the failure percentages are estimated to not be much lower.

Recommendation: Management should ensure that SharePoint system backups are tested periodically to ensure the system can be restored when necessary, and that the time frame expected for full operational recovery can be met. Management should consider requiring annual testing, but the frequency and types of testing performed should be based, at least in part, on the results of a business impact analysis detailing the operational effects of SharePoint being unavailable for a period of time.

Response: SharePoint backups are being evaluated as part of Capital Programs disaster recovery plans.

180118-3

REP