CAPITAL PROGRAMS

CAPSTAR SYSTEM REVIEW

AUDIT REPORT #21-2101

Audit & Advisory Services

April 2021

CAPITAL PROGRAMS

CAPSTAR SYSTEM REVIEW

AUDIT REPORT #21-2101

Background

In accordance with the Campus fiscal year 2020-21 audit plan, Audit & Advisory Services

(A&AS) conducted an audit of internal controls and associated procedures established to operate and safeguard Capital Programs’ (CP) CapSTAR System and its underlying data.

The UCLA CP Information Technology (IT) Unit provides and maintains a local network, hardware, help desk support, software, and several internal web applications. The key IT systems include: 1) CapNET – The primary network backbone supporting all hardware and software needs for users.; 2) Capital Projects Status, Tracking, and Reporting applications (CapSTAR); 3) SharePoint – Server for document management, organization, retention management, and security management; 4) BlueBeam – Server and client application for tracking simultaneous comments on architectural drawings or other PDF documents; and 5) DocuSign – Utilized for the routing of documents for approval and electronic signatures.

CapSTAR is a proprietary software system that was originally designed by CP IT and outside independent software consultants 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 CP senior management. The system is widely used by CP personnel and other capital project development personnel across the University, including users in Housing & Hospitality Services, Facilities Management, and UCLA Health. Since CapSTAR’s inception, there have been multiple system upgrades, with a transition to a web-based platform in recent years. CapSTAR web applications include the following eight applications:

1. Project Initiation – The application is utilized to submit and monitor Project Initiation requests and establish plant account numbers. The application identifies project scope, a preliminary budget, and funding assumptions. It also has a module to submit and track Environmental Impact Classification requests. The Project Initiation website was created in May 2016.
2. Projects – Application designed to record, track, and report data related to UCLA’s capital improvement program and consists of a number of tabs that provide forms for entering, editing, and viewing project information. Project management staff input and maintain project-related data, including budgets and schedules, in the projects module. Project Accounting staff establish new accounts and sub-accounts in this module and use it to edit plant and non-plant jobs. Some enhancements have been made to the projects module, which include change management, contractor pay, meeting minutes, punch list, submittals, transmittals, and warranty.
3. Contracts – Application allows Contracts Administration staff to track the bidding process and other contract-related information, including a vendor list, the contract questionnaire, and contract generation. Contract generation is a powerful feature of the Contracts module, allowing authorized users to generate a variety of mail-merged construction documents or agreements.
4. Inspections – The inspections website was developed in June 2015 to help improve the inspection workflow and timeliness. The website has interfaces that allow contractors to request inspections online; for inspectors to respond to these requests and communicate observations, acceptance, or rejection of specific items required for job completion; and for project managers and construction managers to see how inspections are progressing for their respective projects. The website will also allow the team to document and track how inspection requests were resolved. They have the option to “pass/accept” or “reject/return” the inspections, and move forward with next steps.
5. ePlanRoom – Application provides the ability to view construction plans and documents such as architectural drawings, floor plans, plumbing, HVAC, fire and life safety, and electrical wiring diagrams, permits, AutoCADs, 3-D models, pictures, presentations, and specifications.
6. Timesheets – Application is for employees to record the time worked on projects for recharge purposes. The application has been enhanced due to UCLA implementation of UC Path.
7. Work Flow and Document Management – Application utilized for electronic routing and approval of various construction and administrative processes (e.g., IT purchases, user departures) and key documents. The workflow website was created in March 2017 to replace a limited workflow version in SharePoint. Since its inception, over 7,500 workflows have been completed.
8. Vendor Portal – Allows consultants and contractors to subscribe to receive email notifications about advertisement for bids for UCLA CP projects, prequalification advertisements, and Environmental Impact Requests.
9. Applications – Central location for users to register and request access. A central location for all help files, videos and guides.

The CP IT unit includes an IT Manager, two network administrators and a user support administrator. Outside third-party developers are hired, as needed, dependent on software development requirements. The IT unit reports to the Associate Vice Chancellor of Capital Planning & Finance.

Purpose and Scope

The primary purpose of the review was to ensure that CP’s 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:

* IT Disaster Recovery Plan (DRP)
* Backups
* Environmental Controls
* Backup Power

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

Summary Opinion

Based on the results of the work performed within the scope of the audit, internal controls and associated procedures established to operate and safeguard CP’s CapSTAR System and its underlying data 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:

***IT Disaster Recovery Planning***

To better ensure that critical systems can be recovered in a timely manner to maintain CP’s essential business functions, management should consider the following:

* Capital Programs IT team should work with each of the essential business functions in CP to understand their maximum tolerable system downtime and how promptly these functions need IT systems to be restored to avoid undue operational impact. Once these timeframes have been identified then appropriate IT recovery plans should be established to meet these needs. The IT DRP should be updated and communicated to all applicable personnel. Furthermore, the IT DRP should be reviewed and updated, as applicable, on a regular basis.
* Continue with efforts to identify an alternate systems recovery site.
* The IT DRP should be tested on a regular basis to ensure systems can be recovered within the required timeframes.
* Management should ensure that detailed business continuity plans (BCP) for all of the key CP functions are defined, updated, and documented. In addition, the BCP should be tested on a regular basis to ensure that key functions can continue in the event of a disaster.

***Backups***

* Although IT management indicated that there have not been any issues with restoring data from backups, to better ensure backups can be successfully restored in case of emergencies or other outages, test restores of backups should be performed on a regular basis and the results of such tests documented.

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

Audit Results and Recommendations

IT Disaster Recovery Planning

1. IT Disaster Recovery Plan

The CP department has established and documented an IT DRP, which includes the following components:

1. Disaster Preparation Plan – identifies the actions that have been implemented to prevent and prepare for a disaster including regular backups, environmental controls in the server room, and specifications for replacement computer hardware.
2. Emergency Response – defines the initial actions to take in the event of an emergency, including assessing the situation, responsibilities of the IT disaster recovery team, decisions on how to best restore IT systems, and notifying all applicable CP personnel.
3. Disaster recovery procedures for different scenarios of disruptions:
   * Power Outage Less Than 5 Minutes
   * Power Outage Between 5 to 24 Hours
   * Building Damaged and Only Partially Accessible
   * Building Damaged and Cannot be Accessed

There are some aspects of the IT DRP that can be further enhanced:

* The timing of when numerous CapSTAR modules can be restored is not aligned with the required recovery timeframes indicated by CP business functions in the department’s business continuity plan. The IT DRP has classified two tiers of systems. First tier systems, such as the CapSTAR ePlanRoom, which maintains important building drawings and floorplans, must and can be restored within 24 hours. All other CapSTAR modules have been classified by the IT team as second tier systems with plans to restore these modules within seven days. However, the seven day time frame is not aligned with the recovery timeframe indicated by CP business functions in the BCP, which range from one day to four weeks.
* Previously there was an arrangement to utilize UC Berkeley as a recovery site in the event of a major disaster at UCLA; however, that has been discontinued. Microsoft Azure Cloud services is currently being assessed as an off-site recovery solution starting with the CapSTAR ePlanRoom application and then testing the other CapSTAR applications to determine if they can operate properly in the cloud. Testing was estimated to be completed by the end of 2020 and depending upon the performance and costs, management will decide whether to use Azure Cloud as a backup DRP solution or potentially migrate the local production CapSTAR systems to another cloud service provider.
* Regular testing of the IT DRP is not performed.

Recommendation: To better ensure that critical systems can be recovered in a timely manner to meet the requirements of CP’s business functions, management should consider the following:

* Capital Programs IT team should work with each of the essential business functions in CP to understand their maximum tolerable system downtime and how promptly these functions need IT systems to be restored to avoid undue operational impact. Once these timeframes have been identified then appropriate IT recovery plans should be established to meet these needs. The IT DRP should be updated and communicated to all applicable personnel. Furthermore, the IT DRP should be reviewed and updated, as applicable, on a regular basis.
* Continue with efforts to identify an alternate systems recovery site.
* The IT DRP should be tested on a regular basis to ensure systems can be recovered within the required timeframes.

Response: The IT staff has developed a strategy to move all key websites to an external cloud platform to ensure availability during an emergency.

With the transition to cloud-based applications using Microsoft infrastructure, key systems will be available 24x7 and in the event of a disaster.

* 1. Databases and key websites will be hosted in Microsoft Azure cloud, with minimal possibility of business interruption.
  2. Microsoft Cloud Services have had an uptime of 99.995%. Converted into minutes, that is less than 30 minutes of downtime for the year.
  3. Microsoft Cloud services test their business continuity plans at least annually per Enterprise Business Continuity Management (EBCM) policies. To validate resilience and recovery strategies against a wide range of potential incidents, the EBCM Program defines multiple categories of test scenarios affecting people, locations, and technology. The level of validation required for each service is based on the service’s criticality, with more critical services receiving more rigorous validation.

Transition to a cloud-based infrastructure is a multi-step process, which has included updates to both hardware and software. To enable the migration of SharePoint data to the Cloud, Capital Programs has updated its Cisco network infrastructure. The successful testing of the SharePoint site was completed in the fourth quarter of 2020. Other CapSTAR web applications have also been successfully tested and Capital Programs plans to migrate all CapSTAR sites to the Cloud in the second quarter of 2021. This plan should address all concerns regarding the development of an alternative systems recovery site.

The IT DRP will be tested on an annual basis.

1. Business Continuity Plan

Capital Programs has utilized the UC Ready tool to create an overall business continuity plan for the department; however, for some of the key business functions detailed continuity plans have not been defined completely or have not been recently updated.

* In the event of a business interruption, a detailed strategy to communicate the length of an outage, impact on services, when to report to work, alternate locations, and how to communicate to all applicable stakeholders has not been defined.
* Continuity plans have not been defined in the event of loss of the IT network, workspace, and key personnel for the following business functions: Architectural Design, Plan Room, Building Department, Project Approvals, and Managing Projects and Inspections.

Recommendation: Management should ensure that detailed continuity plans for all of the key CP functions are defined, updated, and documented. In addition, the BCP should be tested on a regular basis to ensure that key functions can continue in the event of a disaster.

Response: In the event of business interruption, communication with staff can occur in the following ways:

* 1. Emails/Text can be sent to individuals describing the emergency and specific steps to take.
  2. Users can access a central SharePoint Emergency Site to obtain the latest news, status, and instructions.
  3. Users can access an emergency phone list on the SharePoint Emergency website to call people for further information.

The Business Continuity Plan (BCP) update was updated in February 2021 by the IT Staff and various stakeholders on a unit-by-unit basis. Regular updates to the BCP will be conducted on an on-going basis and a complete review will be conducted on an annual basis.

Backups

Discussions were held with IT management and relevant documentation was reviewed to verify whether the CapSTAR system is regularly backed up to allow for recovery in the event of data loss. The CapSTAR system is backed up on a daily basis to a local Network Attached Storage (NAS) device and to an offsite location, Microsoft Azure Cloud.

There were no significant control weaknesses noted in this area.

1. Backups - Test Restores

A&AS met with CP IT management and reviewed existing procedures for backups of departmental data. Based on our review, it was noted that procedures for test restores from backups could be enhanced. Currently, restores from backups are only performed as needed.

Recommendation: Although IT management indicated that there have not been any issues with restoring data from backups, to better ensure backups can be successfully restored in case of emergencies or other outages, test restores of backups should be performed on a regular basis and the results of such tests documented.

Response: Backups of data and restoration of backups will be mitigated once Capital Programs migrates to Microsoft Azure Cloud.

Non-key systems that are hosted on premise will continue to have local backups. These on premise backup restore procedures will be tested on a regular basis.

Environmental Controls

Key systems and IT equipment that supports CP’s critical business functions are maintained in the CP building’s server room. The adequacy of environmental controls to ensure the operations and protection of these key systems were assessed, including review of relevant documentation and discussions with IT management.

A&AS noted that the Capital Programs’ server room is adequately ventilated through the building’s central air conditioning system. A backup 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. Additionally, the server room is monitored by a smoke detector/alarm, a fire suppression system, and fire extinguishers for liquids and electrical equipment. Servers, NAS devices, uninterruptible power supply (UPS) devices, and other equipment are maintained in six server racks. Lastly, all server racks contain seismic bracings to prevent movement or injury during seismic activity or an emergency.

There were no significant control weaknesses noted in this area.

Backup Power

Discussions were held with IT management and relevant documents were reviewed to determine whether adequate controls had been established to ensure the continued operation of the CapSTAR applications in the event of power outages. There are UPS devices connected to the CapSTAR system, which provide five minutes of backup power in the event of brief power outages. In the event of extended power outages, the UPS devices provide temporary power to allow for the CapSTAR servers to be safely powered down. Automated biweekly self-tests of the UPS are conducted to ensure that the devices will function properly in the event of power outages.

There were no significant control weaknesses noted in this area.

210203-4

REP