AUDIT & MANAGEMENT
AMAS
ADVISORY SERVICES

Audit Report

ITS Change Management

Report No. SC-20-01
June 2020

Auditor In Charge
James Dougherty

Approved
James Dougherty, Director
Audit & Management Advisory Services

UC SANTA CRUZ

Table of Contents

I. EXECUTIVE SUMMARY

Audit and Management Advisory Services (AMAS) has completed a review of ITS Change Management to evaluate its effectiveness and efficiency in achieving its goal of managing changes to the production environment by minimizing impact and reducing the risk of unintended service disruptions. This audit was included on the campus FY 2019-20 internal audit plan.

While ITS has a change management process, we do not believe it is developed to a level where it can achieve the best effective and efficient changes that ITS is capable of. This is partially because when ITS created its current iteration of change management that made use of a sophisticated software platform, its use was not required. Consequently, there are different methods by which change is managed and even areas where change takes place without a standard change management process.

We believe that ITS can improve its change management, but will have to begin with support from its senior management to ensure it is adequately resourced and the division understands what change management process they need to implement. This is an iterative process that will require project management over time.

The following observation requiring management corrective action is identified below:

ITS Change Management Maturity

The ITS Change Management process is not mature enough to achieve its goal of ensuring that only approved modifications to the environment are implemented.

Agreement was reached with management on the recommended action to address the risks identified in this area. The observation and the related recommendation are described in greater detail in section III.

II. INTRODUCTION

Purpose

The purpose of the review was to evaluate the ITS change management process and determine how effective it is in meeting its objective of managing changes to the production environment by minimizing impact and reducing the risk of unintended service disruptions.

Background

Information technology (IT) change management can be a complex and difficult process to implement and maintain. It requires collaboration among cross-functional teams throughout an organization, and its success or failure can have a significant impact on an organization's operations. As technology advances and organizations move from manual to automated and digital processes and cloud applications, the number of processes subject to change management will only increase. In addition, the need for these systems to function properly with appropriate and effective controls, will be of utmost importance.

Change management controls are an integral part of an organization's IT general controls[1]. In most organizations, the question isn't whether a change management process exists; it's whether the process is as effective and efficient as possible and is followed for all changes. Generally, effective change management can assist an organization in addressing risk, reducing unplanned work, limiting unplanned downtime, and ultimately improving the quality of service for internal and external customers.

According to ITIL[2], a leading standard in service management, "Change is the addition, modification, or removal of anything that could have a direct or indirect effect on services. Its scope includes all IT infrastructure, applications, documentation, processes, supplier relationships, and anything else that might directly or indirectly impact a product or service."

The goal of change management in an IT environment is to ensure that change requests (including emergency changes) are handled quickly, efficiently, and effectively. This goal is accomplished by following consistent procedures and maintaining them in a controlled manner. This systematic approach improves business operations by reducing the potential of issues related to confidentiality, integrity, or availability. Properly implemented, change management protects the production environment ("live" environment) and provides the organization with a repeatable, measurable, and auditable process that captures all technology-related changes.

Scope

Our scope was limited to ITS Change Management during FY20. We conducted this review by means of the following:

- Reviewed various standards on IT change management including ITIL and COBIT.
- Review UC policy on IT change management, specifically BFB IS-3.
- Reviewed ITS Change Management website information, including the ITS Maintenance Calendar.
- Reviewed a previous UCSC audit on change management "ITS Change Management SC-11-11."

[1] University of California Policy BFB IS-3 Electronic Information Security, Section 12.1.2 Change Management
[2] ITIL was formerly an acronym for Information Technology Infrastructure Library, but it is no longer used as an acronym.

- Interviewed ITS managers to gain an understanding of change management in ITS.
- Performed and documented a risk assessment based on the results of our preliminary work, such as interviews, review of documentation, and other observations.
- Obtained an account in IT Request to review examples of changes documented there.
- Detailed testing that included selecting 15 change requests and related changes including standard, normal and emergency changes.
- Detailed testing included an evaluation of:
    - Communication of the change management process
    - Separation of duties
    - Change management procedures
    - Emergency change
    - Monitoring and reporting

For additional details, please see Appendix A. Summary of Work Performed and Results.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A.	ITS Change Management Maturity	
The ITS Change Management process is not mature enough to achieve its goal of ensuring that only approved modifications to the environment are implemented.		
Risk Statement/Effect		
Changes to ITS managed information or technology may result in outages due to insufficient risk and impact analysis.		
Agreement		
A.1	The ITS Chief Technology Officer (interim) Technology Engineering will make the case to the ITS Senior Management Team for a project to mature ITS Change Management to be able to achieve its goal of ensuring that only approved modifications to the environment are implemented.	**Implementation Date** March 31, 2021 **Responsible Manager** Chief Technology Officer (interim)

A.– ITS Change Management Maturity Detailed Discussion

We are providing here a list of observations that have contributed to the overall observation of ITS Change Management's inadequate maturity. We have organized our observations in this way because they are interrelated in such a way that acting on one will require also acting on others. Developing the maturity of this process will require an iterative strategy as the desirable level of maturity cannot be achieved all at once. We believe that this effort will require support from the ITS Senior Management Team, and project management principles.

More Than One Change Control Process

ITS acquired ServiceNow, a software product that ITS uses for various functions, including its change control module; ITS renamed this software "IT Request." However, its use was not required from the start, which has resulted in several forms of change control implemented by ITS units and departments. This undermines the effectiveness of the ITS Change Management process.

One process in effect before IT Request was acquired is an email notification network, named after the email address: sc.update@ucsc.edu. The ITS change manager is included in this network and enters the change notification in the ITS Maintenance Calendar. In our opinion, while sc.update can continue to be used for communication purposes, it should not be used in lieu of IT Request for changes. Best practices would indicate a single tool for system of record, which here would be IT Request.

There are other ITS areas that do not use either IT Request or sc.update, and may not have any standard change management process.

Formal Training

Training is needed for anyone who is expected to use IT Request for change management. However, no formal training in the use of this tool is provided by ITS. Training should also include the explanation of the purpose of change management and address employee concerns. This would include a clear description of what changes should be managed by the ITS process.

Standard Changes

There are three types of changes: standard, normal and emergency changes. Standard changes are routine, low risk changes with a history of success. Standard changes use templates created by subject matter experts and approved by the change manager. As no further approval is required, and most of the information required by the change request form is already included in the template by experts, these change requests are quick to implement. However, the change manager needs to be confident that the implementation will be successful. IT Request provides statistics of the use of each template for the change manager to monitor. If such changes create issues, then the templates may need to be modified or replaced. Currently, the change manager has not monitored these templates. One reason for this is that users have not been required to evaluate how changes went.

A further factor in ensuring standard changes are reliable is the quality and consistency of their implementation, which may require management to ensure implementation of the template instructions is carried out accordingly and may require an investigation of the requirement, development, testing and quality assurance processes of the organization. If there is resistance to the use of IT Request, employees may attempt to circumvent the process by choosing a Standard Change template to get their change implemented without going through the change manager's approval even though their change does not qualify for this change type.

Post Implementation Review

A post implementation review (PIR) field exists in IT Request where those implementing the change can document what they learned from the change, such as whether successful or not. Further, if a change creates problems and generates incidents reported in IT Request, these can be linked to the change that caused the incidents. Currently, users are not required to fill out PIRs. In our sample of IT Request changes we analyzed, there were no incidents in the Incident field that were caused by any of the changes. This might be normal as we would not expect to see many changes result in incidents, but it may not be required to connect incidents with changes currently. We saw an example of a change that produced an incident but this was not recorded in IT Request. PIRs should be filled out after emergency changes to ensure that emergency procedures were justified.

We recommend that a formal post-mortem be documented within five days of an incident where a formal post-mortem was requested or warranted, and the post-mortem document be attached to the change ticket. Actions completed need to be updated on the document and updated on the change.

Separation of Duties

Separation of duties is the effective collection of requirements, coding (w/ peer/QA reviews), testing and approval by all parties impacted by the change. Most importantly, separation of duties minimizes the potential for the change to be modified at the last minute that may increase risks to campus operations or allows someone to make a change that compromises campus assets. Depending on the change, it may move from one environment to the other, such as migrating from development to testing to user testing and finally to production. To protect the production environment, changes should be managed in a repeatable, defined, and predictable manner. Care

should be taken to ensure changes made to correct one application, server, or network device do not have unintended consequences on other devices or applications.

IT Request identifies four different roles in the change request: "Requested by", "Opened by", "Assigned to" and "Release Manager". The Assigned to is the person who executes and completes the change management process and has overall responsibility for successfully completing the change. This person should be different from the person who requested the change and the person who opened it. This was not always followed in our sample of changes and is an indication that separation of duties may not always be followed. We believe this to be a training issue in the proper use of IT Request.

There are exceptions regarding adequate separation of roles, such as when a change is not managed by ITS. For example, changes to UCPath that are managed by UCOP or changes to other campus systems managed by different campus divisions are reported to ITS through sc.update. There are also occasions when the same person opening a change will be assigned to implement it due to a shortage of qualified personnel to implement the change. In these cases, other mitigating controls should be in place.

The release manager is responsible for production software, hardware, or a combination of both where an approved change finally takes place.

Open Changes

There were a large number of open changes (124 as of 6/16/2020) beginning with a changed scheduled for January 2019 to the present. We believe that among them are changes that should have been closed but were not. This is a training issue as well as a monitoring one.

Monitoring and Reporting

In a standard IT change management process, metrics are gathered and reported to higher management for their evaluation of the process. IT Request metrics are not currently taken or reported. This is mainly due to the low level of ITS Change Management maturity.

Common metrics collected for the change management process include:

- Total number of changes for a set period.
- Changes that were successful.
- Success or failure of rollback plans.
- Changes that deviated from the defined change management process.
- Percentage of emergency changes.
- Number of outages during a set period.
- Percent of unplanned work of total work performed by IT personnel.

Support for ITS Change Management

Currently there is one change manager with one or two backups. The change manager position is not 100 percent time; change management fills a portion of the employee's time. Normal change requests are taken twice a week. If all information and technical changes managed by ITS go through a single process, this will require more time from the change manager. Standard changes should be encouraged so the change manager only needs to review normal and emergency changes.

We can expect that those who use IT Request for changes will need more support than formal training. They will have questions and will need further help using the platform. Also, they will need to understand the function of the change manager. This function is to ensure a risk and impact analysis has taken place that will prevent the change from adversely impacting other systems. The change manager does not have to be an expert in all the changes to ask the right, risk-related questions that extend thinking beyond technical siloes.

****

APPENDIX A. SUMMARY OF WORK PERFORMED AND RESULTS

Preliminary Analysis	
Work Performed	**Results**
Reviewed standards for change management, UC policy and ITS Change Management website information.	1. Standards: • ITIL Foundation 4 Edition • COBIT 2019 • IIA GTAG Change Management 2. UC Policy BFB IS-3 Electronic Information Security 3. ITS Change Management website: Contains explanation of the process, how to use IT Request for changes, and various types of change and responsible parties. It also includes the ITS Maintenance Calendar.
Reviewed previous audit of ITS change management	SC-11-11: This provided a point to compare ITS change management then and now.
Interviewed Chief Technology Officer (interim), Client Support Manager, and Change Manager	Developed a risk matrix and audit program to address the risk areas identified.

Fieldwork	
Work Performed	**Results**
We reviewed various risk areas by taking a sample of change requests and related changes and interviewing ITS personnel to gain a better understanding of what we were seeing and implications.	
Selected 15 samples of open changes for review.	• Of 13 change requests that were either in implement or complete stages, 11 had the same person in request by, opened by, and assigned to fields; one of these was also the release mgr. • Two samples of emergency changes did not have record of CAB approval in IT Request, nor did they have a post implementation review in IT Request.
We had meetings and correspondence with the Service Manager, Change Manager, the Chief Information Security Officer, the Director of Software Engineering, Technology Engineering, and the interim Director of the Network Infrastructure and Operations Manager.	Much useful information was gathered that is in the report.
Communication of Change Management: 1. Interview chief technology officer and current change manager and her backup. 2. Review ITS Change Management website.	1. Interviewed the chief technology officer about communication of CM process. 2. Reviewed CM website for description of process. 3. Interviewed CM manager if training in the CM process was provided to ITS personnel.

Fieldwork	
Work Performed	**Results**
Separation of Duties: 1. Validate that changes are reviewed and approved by an appropriate level of management. 2. Validate that change approvers do not have access to implement changes in the production environment. 3. Determine how changes are tested to ensure they function as intended and do not impair the integrity, availability, or confidentiality of data.	1. A change manager is assigned as well as a back up who provides approvals. 2. A change manager has access to implement changes in the production environment, however, the backup change manager provides approvals should the change manager request a change. 3. Changes are commonly tested in a production equivalent environment. 4. The person assigned to the make the change should not be the person requesting or opening it, but this happens due to limits of the number of employees with necessary skills to make the change.
Change Management Procedures: 1. A standard and centralized process exists for processing all changes. 2. All changes are approved by the appropriate level of management 3. All changes are categorized and assessed for impact.	1. A standard and centralized process exists for processing all changes. 2. There is an approval process, but change management does not believe all changes go through this process. 3. Changes recorded in IT Request include change category and assessment. 4. Changes in IT Request are tested prior to implementation into production. 5. Changes in IT Request are scheduled and communicated prior to implementation. 6. Rollback/backout plans are considered for IT Request changes, but may not be needed if the change is simple.
Emergency Changes: Select a sample of emergency changes and validate that they meet the definition/criteria of a genuine emergency change and that proper controls were performed from initiation through implementation for each.	1. Changes that occur during change restricted periods are emergency changes. 2. Samples demonstrated approval from a central approval board (CAB), the ITS senior management team. This approval was not documented in IT Request. 3. We did not see a post implementation review process to verify that the change qualified as emergency.
Monitoring and Reporting:	Metrics of change management are not kept and reported to ITS higher management.

Fieldwork	
Work Performed	**Results**
1. Determine what metrics exist, how they are calculated, and by whom. Identify to whom they are reported 2. Determine whether the metrics are appropriate, complete, and accurate. 3. Common metrics collected for the CM process include: • Total number of changes for a set period. • Changes that were successful • Success or failure of rollback plans.	