UNIVERSITY OF CALIFORNIA, DAVIS
AUDIT AND MANAGEMENT ADVISORY SERVICES

UC Davis
Review of Prior Years' MCAs
Audit & Management Advisory Services Project #19-11

June 2019

Fieldwork Performed by:
Ryan Dickson, Audit Manager

Reviewed and Approved by:
Leslyn Kraus, Director

Review of Prior Years' MCAs
AMAS Project #19-11

MANAGEMENT SUMMARY

Background

When a report issued by AMAS makes a finding of moderate to high risk, operational management over the area at risk is asked to provide language describing action that will be taken in response. This language is incorporated into the report as a Management Corrective Action (MCA). AMAS provides follow-up and accountability during the corrective action process, and closes the MCA once its language has been satisfied.

Sometimes the action to be taken is significant and will require more time than allowable during the MCA follow-up process.[1] In these cases we may accept a plan for action, rather than the action itself, as evidence that the risk is being addressed.

As part of the fiscal year 2019 audit plan, we revisited selected high-risk Management Corrective Actions (MCAs) that had been closed based on documentation of a plan for action.

Purpose and Scope

The purpose of this audit was to verify that plans submitted in response to moderate and high-risk findings have been implemented.

In order to accomplish this objective we interviewed management responsible for plans, and reviewed supplemental documentation.

This audit reviewed five MCAs that had been closed during fiscal years 2014 - 2018.

Conclusion

We were able to verify that for each of the plans selected, at least some progress had been made. In four cases we determined that additional action would be necessary to mitigate the underlying risk.

Please see the table on the next page for the original MCAs, a brief status update, and new MCA language that is being issued as a result of this review.

[1] MCAs must be closed within 300 days of issuance of a final report.

Project	Original MCA Language	Status Update	New MCA Language
14-29 IET Virtualization Service	B.1 IET will develop a risk management practice that includes a schedule for performing periodic risk assessments for the virtualization environment. With guidance from applicable laws, regulations, UC and UCD policies governing data protection, VM clients are responsible for determining if it is appropriate to host protected or high-risk data in their VM instances and this responsibility will be documented in the SLA. IET will work with its clients to identify protected and high-risk data hosted in the VM environment and determine if existing security controls are sufficient to safeguard the client's protected or high-risk data.	IET is developing processes to identify high-risk data upon receipt at the Data Center; to catalog current data stored in the Data Center according to BFB-IS-3 §8; and to schedule risk assessments of the Data Center and virtualization emvironment.	By March 31, 2020, IET will implement a process for cataloging new data at intake and initiate a complete inventory of data housed in the Data Center. The CISO will schedule risk assessments of the Data Center and virtualization environments.
16-10 Research Data Security	In consultation with the research data advisory group, the Chief Information Security Officer (CISO) will expand the university's information security risk management program to address research data security risks across the University. 16-10.2.a: The enhanced program, will at a minimum include: * Criteria to evaluate research data security risks. * A process to work with the Office of Research, and the Institutional Review Board (IRB) for collecting and sharing information on contracts processed by their office to ensure high risk research projects are being identified early and consistently communicated to the CISO for inclusion in the enhanced risk management program. * A risk register for research data risks across the University that are identified during the assessment process. 16-10.2.b: Establish a process to engage IT resources to develop and implement security plans for research data for research projects identified as having high risk research data. 16-10.2.c: Establish and implement a partnering relationship with Campus Unit IT personnel in the Colleges and Schools excluding units supported by UCDHS to assist with the identifying, conducting, monitoring, and reporting on research project risk exposures.	In collaboration with SPO, the CISO's office is actively involved in conducting risk assessments of select research projects. Typically, an assessment is performed when SPO identifies security provisions that need further investigations or when the CISO is required to sign an attestation of security controls. This process is not documented in a memorandum of understanding, service level agreement, or similar format. Nor does this process provide a mechanism for review of research performed at the School of Medicine.	By March 31, 2020, the CISO will work with the Office of Research to finalize a statement of intent, which will define responsibilities related to formal assessments of research data security risk. This document will describe procedures for identification of high-risk research projects, assessment by the Information Security Office, and response by the Office of Research. It will cover research administered through both the Davis and Sacramento campuses. It will be signed by the CISO and the Executive Director for Sponsored Programs.
16-17 Associated Students, University of California Davis (ASUCD)	Between November 2015 and February 2016, ASUCD will take steps necessary as required by ASUCD bylaws to establish an Auxiliary Business Governance Board (Governance Board). [...] After having been established, the Governance Board will consider the recommendations included in this report and take the following actions and/or ensure that ASUCD personnel take the following actions to address the issues identified in the report.	ASUCD was not able to recruit board members as required in the MCA. It is developing an Executive Council that will serve the same function.	By March 31, 2020, ASUCD will finalize bylaws for an Executive Council. That council will be formed and hold an inaugural meeting.
17-07 Institutional Data and Security	d: The IET-Banner Unit Information Security Coordinator working with the CISO will establish a plan and schedule risk assessments (including developing a security plan) for the Banner high-risk institutional data systems. e: The FOA Unit Information Security Coordinator working with the CISO will establish a plan and schedule risk assessments (including developing a security plan) for the KFS high-risk institutional data system. f: The FOA Unit Information Security Coordinator working with the CISO will establish a plan and schedule risk assessments (including developing a security plan) for the CDW high-risk institutional data system. g: The DEVAR Unit Information Security Coordinator working with the CISO will establish a plan and schedule a risk assessment (including developing a security plan) for the AIS high-risk institutional data system.	The CDW assessment is nearly done. KFS, AIS, and Banner are planned to be addressed as part of a BFB-IS-3 deployment project.	By March 31, 2020, the CISO will complete risk assessments for the KFS and AIS. These assessments may take a more tailored or focused form than typical of those performed by the Information Security Office. The Banner system will be revisited by AMAS during a FY20 Administrative Review of IET.