SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

August 21, 2012

DAVID BRENNER, M.D.
Vice Chancellor
Health Sciences
0602

ED BABAKANIAN
Chief Information Officer
Health Sciences
8983

Subject: ***Health Sciences Enterprise IS-3 Compliance Review***
Audit & Management Advisory Services Project 2012-13

The final audit report for Health Sciences Enterprise IS-3 Compliance Review; Audit Report 2012-13 is attached. We appreciate the cooperation extended by Health Sciences personnel who participated in the audit process.

Because we were able to reach agreement regarding corrective actions to be taken in response to the audit recommendations, a formal response to the report is not requested.

The findings included in this report will be added to our follow-up system. While management corrective actions have been included in the audit report, we may determine that additional audit procedures to validate the actions agreed to or implemented are warranted. We will contact you to schedule a review of the corrective actions, and will advise you when the findings are closed.

UC wide policy requires that all draft audit reports, both printed and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel, or destroy them at this time.

Terri Buchanan
Interim Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: R. Espiritu
G. Matthews
S. Vacca
K. Wottge

AUDIT & MANAGEMENT ADVISORY SERVICES

University of California
San Diego

UC San Diego Health Sciences Enterprise
IS-3 Compliance Review
August 2012

Performed By:

Jennifer McDonald, Auditor

Approved By:

Terri Buchanan, Interim Assistant Vice Chancellor

Project Number: 2012-13

UC San Diego Health Sciences Enterprise IS-3 Compliance Review
Audit & Management Advisory Services Project 2012-13

Table of Contents

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of University of California San Diego (UC San Diego) Health Sciences Professional Schools[1] (Professional Schools) and Health System[2] (Health System) compliance with Business and Finance Bulletin IS-3, *Electronic Information Security* as part of the University of California systemwide review included on the approved audit plan for Fiscal Year 2011-12. This report summarizes the results of our review.

The University of California (UC) is committed to a high standard of excellence for the protection of information assets and information technology resources that support the University enterprise. The University processes, stores, and transmits a large amount of electronic information to conduct its academic and business functions. Appropriate controls and security measures are essential to protect information assets from being subjected to potential damage or compromise, affecting confidentiality and privacy and possibly interrupting critical University activities.

UC Business and Finance Bulletin IS-3 *Electronic Information Security* (IS-3) establishes guidelines for protecting University electronic information resources, and identifies the roles and responsibilities for complying with the guidelines for personnel that use UC computer systems. IS-3 applies to the Office of the President (UCOP), all UC campuses and Medical Centers; the UC managed Lawrence Berkeley National Laboratory; and other University locations (campuses[3]). The following general topics are addressed in IS-3:

- Information Security Program
- Minimum Requirements for Network Connectivity
- Major Responsibilities

UC San Diego has implemented local campus policy PPM135-3: *Network Security* to facilitate compliance with IS-3 requirements. Exhibit B: *Minimum Network Connection Standards* (Minimum Standards*)* provides local guidelines that assist UC San Diego network administrators and systems support personnel with meeting their obligations.

To gauge the strength of information security practices across the UC system, UC Chief Information Officers and the information security community completed an IS-3 self-assessment in Fiscal Years 2007, 2008, and 2009. Responses from the ten campuses,

[1] Health Sciences Professional Schools includes the School of Medicine, the Skaggs School of Pharmacy and Pharmaceutical Sciences, and associated basic and clinical research operations.

[2] The Health System encompasses patient services provided at the UCSD Medical Centers, Hillcrest and La Jolla (Thornton Hospital); the UCSD Moores Cancer Center; and other affiliated healthcare organizations, and primary and specialty practices of the UCSD Medical Group faculty physicians.

[3] This reference includes all University business locations.

five Medical Centers, Agriculture and Natural Resources, and UC Office of the President (UCOP) were consolidated into an overall assessment of system wide IS-3 compliance, which was reported to the UC Regents. In November of 2009, UC San Diego Administrative Computing and Telecommunications (ACT) conducted an online survey to measure the campus compliance with IS-3 and campus electronic security polices and guidelines. The Professional Schools participated in this assessment using the same survey tool, while the Health System completed a different survey that gathered similar information. The compiled 2009 survey results were reported to UCOP and the UC Regents.

A UC systemwide IS-3 audit was performed by UC Internal Audit Departments in March 2011. The review was conducted to provide an independent assessment of IS-3 compliance for each of the 10 UC campuses, the UC Office of the President, and Lawrence Berkeley National Laboratory. Health Sciences and Health System computing environments were excluded from the scope of the 2011 review. A separate IS-3 compliance assessment of those environments was subsequently included on the Fiscal Year 2011-12 audit plan.

Information Technology (IT) Operating Environments

Historically, Health System (Medical Center and Medical Group) IT operations have been managed centrally by the Health System Information Services (IS), led by the Health System Chief Information Officer (CIO). The Health System network is a segment of the campus network backbone, separated by a stately firewall device. Virtual Private Networks (VPNs) have been established, as needed, to provide secure pathways to external users, and network scanning solutions have been deployed to ensure that devices are appropriately configured. Because the Health System generates and stores protected health information (PHI) subject to Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations, a central management structure was developed to allow IS to implement policies, practices and standard technologies needed to effectively comply with applicable regulations.

Campus based users in the Professional Schools (School of Medicine and Skaggs School of Pharmacy and Pharmaceutical Sciences) connect to campus network resources to facilitate business, teaching and research computing needs. With some exceptions, including student information subject to Family Education Rights Privacy Act (FERPA) data security requirements, the campus network was designed to be an open environment to facilitate electronic communication between UC San Diego faculty, staff and students and internal or outside parties without extensive security measures.

Departments and other business units in the Professional Schools may be located on or off campus, and are distributed geographically. As a result, remote operations may assign staff to support local computing equipment and programs; or alternatively, they may rely on a central group based in the School of Medicine Dean's Office (SOM), campus Academic Computing Services (ACS) or another department.

To provide a consistent IT management structure for Health Sciences, the responsibilities of the CIO were expanded to include oversight of all IT and telecommunications infrastructure and management processes across the Health System and the Professional Schools in January 2010. Since that time the Health Sciences and Health System IS departments have combined efforts to establish a common framework to improve the quality and consistency of IT services, and promote the use of standard computer security technologies to distributed Professional School business and research units. IT initiatives have included the establishment of a Work Group that was tasked with identifying the assets and users connected to various computing environments, as well as addressing alternative IT solutions for business and research units that required special considerations based on their computing needs.

II. Audit Objectives, Scope, and Procedures

The objectives of our review were to assess compliance with IS-3 requirements for a sample of Professional School departments and business units, and Health System IS; and based on that assessment, determine if additional local initiatives were needed to mitigate residual regulatory risk within centralized and distributed computing environments.

During the preliminary survey phase of the review, a risk assessment was completed using AMAS' Computer Environment Internal Control Questionnaire (ICQ) and follow-up interviews with key personnel to identify IS-3 and related campus PPM 135-3 policy requirements that had not been fully implemented. The ICQ included questions to help assess the level of compliance with the following IS-3 and PPM 135-3 Minimum Standards network administration and security requirements:

- ✓ Security Education and Awareness Training
- ✓ Identity and Access Management
- ✓ System and Application Security
- ✓ Network Security Tools and Practices
- ✓ Application Systems Management
- ✓ Collection, Management and Analysis of Log Data
- ✓ Data Protection and Encryption
- ✓ Access Controls to Authenticate and Authorize Users
- ✓ Asset Inventory and Classification
- ✓ Risk Assessment
- ✓ Information Security Plan
- ✓ Workforce Administration
- ✓ Physical Security/Environmental Controls

- ✓ Incident Response Planning and Notification Procedures
- ✓ Risk Mitigation Measures
- ✓ Third Party Agreements

Based on the risk assessment results, the review was focused primarily on Health Sciences and Health System IT security governance[4].

We completed the following audit procedures to achieve the project objective:

- Reviewed IS-3 and campus PPM 135-3, the UCSD Minimum Network Connection Standards (Minimum Standards);

- Assessed prior network security audits to identify areas of risk and review corrective actions;

- Evaluated the 2009 IS-3 survey results to assist with the selection of IT environments to include in preliminary survey;

- Interviewed the Health System Information Security Officer (ISO) to understand the current security initiatives occurring within Health Sciences;

- Interviewed the Health System Recruitment Manager and the Health System Human Resource Record Manager to discuss their respective responsibilities as they relate to IS-3 requirements;

- Evaluated ICQ responses and additional supporting documentation to obtain an understanding of network security practices for the 12 IT environments selected for focused review.

- Interviewed department IT staff who completed the ICQ to obtain additional insight into departmental IT security practices; and,

- Completed a detailed matrix of observations across the 12 IT environments assessed (***Attachment A***).

The IS-3 assessment performed during this review was intended to identify the extent to which compliant electronic information security processes and technologies had been incorporated into selected IT environments. Detailed testing of network security controls and processes was not performed within the scope of this review.

[4] IT security governance is the system by which an organization directs and controls IT security. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Governance ensures that security strategies are aligned with business objectives and consistent with regulations

III. Conclusion

We concluded that the CIO and the ISO have taken the appropriate steps to initiate a comprehensive assessment of the Professional Schools IT accountability framework. Additional evaluation should be performed to ensure that there is a consistent strategy for incorporating IS-3 information security measures into IT management practices in all locations. We noted that IT resources were managed by different service centers or staffing models based on department or unit needs and/or location. As additional department/unit IT assessments are performed, there may be additional outreach opportunities to improve the coordination of IT services and improve collaboration between IT administrators and the ISO. Improved collaboration and the establishment of consistent operating standards would assist with assessing centralized and distributed computing support needs; and establishing a foundation to further implement security processes to safeguard information technology resources.

A high level summary of IS-3 assessment observations across the 12 departments and/or business/research units selected for review is provided in ***Attachment A***.

IV. Observation and Management Corrective Actions

A. IT Security Governance

Ongoing assessment of the Professional Schools IT security environment should continue to ensure that resources are sufficient, and comply with the IS-3 requirements for electronic information security. In addition, there may be opportunities to more effectively leverage existing IT resources and service units to provide a consistent level of service to faculty, staff and students.

The ideal IT *organizational structure* would be one that provides clear responsibility, authority, and individual accountability for achieving IT management and security objectives at every level of the organization. The structure would start with a single executive with responsibility for the security program as a whole; and a cognizant security officer who would provide oversight of, and outreach to all IT support personnel, as well as lead committees and work groups in the support of a consolidated security effort; and report to senior management on the overall state of IT security. Finally, the roles of all IT security committees and work groups would be clearly defined.

Health Sciences CIO and ISO responsibilities were consistent with this model, and since January 2010, they have been meeting with Professional School department Chairs and Business Officers to understand and help to assess the current IT environments.

Based on the ICQ responses received, AMAS identified that the source of IT technical support and security management varied by department and unit. Some areas opted to purchase services from one or more of the following service providers:

- SOM IT (two of 12 departments/units business offices);
- Health System IS (one clinical department of 12 departments/units); and
- A combination of services from SOM IT, Academic Computing and Media Services, Pharmacology, or IS (remaining areas of 12 departments/units)

During project fieldwork, we also noted that six of the 12 IT computing environments reviewed were administered by dedicated IT support staff or designated individuals[5] within each respective unit. In some cases, information gathered up to that point was not sufficient to assess whether IT personnel at the department/research unit level had the technical skill set needed to implement and support effective security services; or whether the IT environments were operating in full compliance with IS-3 and Minimum Standards. As a result, Health Sciences executive leadership and the CIO have made available new resources which were engaged in conducting department IT assessments. The ISO indicated that these resources will be continuously engaged with departmental IT staff to ensure compliance with the Universities policies.

In addition, we were advised by management in one department that its business office was completing an IT security self assessment of its research computing environment(s) to help address security concerns and support issues. Self assessments of this type will provide valuable information to the ISO's assessment process.

If collaboration has not been established between interrelated network management and security resources that report to different departments, divisions or researchers, process inefficiencies or miscommunication may occur. Greater transparency in the IT support infrastructure and computer services delivery models across Health Sciences operations will help to provide clear responsibility, authority, and individual accountability for achieving security objectives.

Management Corrective Actions:

1. Under the direction of the CIO, the Health System ISO is coordinating an evaluation of the Health Sciences computer

[5] Individuals within the department or unit tasked with IT responsibilities but without proper IT experience or training.

network and data security program to identify the current support structure and critical areas of operation.

2. The CIO will continue efforts to assess and re-design the IT accountability structure and the computing services delivery model to promote clear responsibility, authority, and individual accountability; and the technical tools needed to achieve security objectives across the Health Sciences domain.

3. To effectively guide that effort, the ISO will develop a plan to eliminate existing gaps in IS-3 compliance based on observations noted in ***Attachment A*** with target timelines for completion. The plan should include programs for:

    - A cohesive organizational structure aligning responsibility and authority for effective enterprise computer security management;

    - An ongoing risk assessment process that includes participation by all areas of the Health Sciences enterprise, and provides measures to address risks in a timely and effective manner;

    - Written guidance (policies, procedures, standards, implementing guidelines, etc.) for management and department network administrators;

    - Effective education and training for all management and staff with computer security responsibilities;

    - Adequate monitoring, auditing, and enforcement mechanisms to identify and correct root causes of security weaknesses in high risk circumstances; and

    - Optimized use of appropriate technical solutions (software and hardware), to address technical security issues.

Audit & Management Advisory Services
UC San Diego Health Science Enterprise IS 3 Compliance Review, Project 2012-13
IS-3 Assessment by Policy Requirement
Attachment A

Assessment Categories	Objective	Observations
Management Measures: People		
1. Security Education and Awareness Training	Assess employee's awareness of system-wide security policies.	Three of 12 units reported awareness of campus training programs, but IT personnel had not attended training sessions. One unit did not have any formal technical or policy training.
Technical Measures		
2. Identity and Access Management	Assess the technical measures for controlling authentication and authorization (password policy, access rights/roles).	All units reported that campus AD or Ldap mechanisms were in place. One unit supported standalone devices with single authentication mechanisms.
3. Systems and Application Security	Assess the procedures in place for systems responsibilities including separation of duties; backup and retention efforts; and patch management practices.	Two of 12 units reported that a comprehensive process for providing systems and application security was not in place. In particular, workstations were not actively managed.
4. Network Security Tools and Practices	Assess the network security strategies and technical security measures (Minimum Standards for Network Connectivity).	Three of 12 units did not employ dedicated IT support staff or procedures performed by an IT service unit to ensure compliance with Minimum Standards.
5. Application Systems Management	Assess the process for application version control and migration practices from development to quality assurance to the production environment. Assess the change management practices for software development and configuration.	The majority of software development was occurring within one SOM business unit. Separation of duties and change management controls were not in place for application development activities.
6. Collection, Management and Analysis of Log Data	Assess the audit log infrastructure and review practices.	All units reported that system audit logs were generated. However, it was not possible to conclude that logging practices conformed to Minimum Standards requirements.
7. Data Protection and Encryption	Assess the use of encryption for data in transit and data at rest.	Two units reported that restricted data was not encrypted. Three of 12 units utilized SOM IT server management resources. SOM IT was in the process of researching data encryption options at the time of our review.
8. Access Controls to Authenticate and Authorize Users	Assess the controls for session protection, automatic logout, and procedures for managing privileged accounts.	Based on survey responses, access controls appeared to be adequate across the 12 units assessed. Further validation will provide assurance of proper account provision.
Management Measures: Processes		

Audit & Management Advisory Services
UC San Diego Health Science Enterprise IS 3 Compliance Review, Project 2012-13
IS-3 Assessment by Policy Requirement
Attachment A

Assessment Categories	Objective	Observations
9. Asset Inventory and Classification	Assess the process for identifying electronic information resources.	Seven of 12 units reported that asset inventory and classification processes had not been conducted, were not complete, or had not been updated.
10. Risk Assessment	Assess the process to understand and document the risks in the event of failures that may cause loss of confidentiality, integrity, or availability of information resources. Identify the level of security necessary for the protection of the resources	Ten of 12 units reported that a formal IT risk assessment had not been completed.
11. Information Security Plan	Assess the departments documented process for accepting a level of risk for systems and processes, and that procedures and controls in place will enhance the security of information assets.	Ten of 12 units reported that a formal, comprehensive security plan had not been developed.
12. Workforce Administration	Assess the process for granting and/or revoking, authorizing and protecting access to information systems.	Five of 12 units reported that there was no formal process in place for granting and/or revoking access to information systems.
13. Physical Security/Environmental Controls	Assess the procedures for physical protection of resources that support restricted or essential systems and/or data.	Seven of 12 units reported using SOM IT server management resources. Two reported using San Diego Super Computer for server location; two reported using HSIS for server location; and one reported having a dedicated server room with proper environmental controls.
14. Incident Response Planning and Notification Procedures	Assess the process for reporting and handling a security incident.	All 12 units reported having a formal process for incident response notification.
15. Risk Mitigation Measures	Assess the process for prevention, detection, and recovery from emergency conditions.	Seven of 12 units reported using server support resources in SOM. Two reported housing file servers at the San Diego Super Computer Center; two reported housing servers at the Health System Kearney Data Center; and one reported having a dedicated server room with proper environmental controls.
16. Third Party Agreements	Assess the process for purchasing standards with respect to assuring proper safeguards of University information resources.	All 12 units used central purchasing departments for procurement. Evaluation of the central purchasing process was not included in the scope of this review.