UC RIVERSIDE: AUDIT & ADVISORY SERVICES

Date: June 30, 2011

To: Charles Rowley, Associate Vice Chancellor
Computing & Communications

Subject: Systemwide Audit – Electronic Information Security – BFB IS-3

Ref: R2011-14

We have completed our audit of Electronic Information Security – BFB IS-3 as part of a systemwide audit effort under the direction of the University Auditor's Office. Our report is attached for your review.

We will perform audit follow-up procedures in the future to review the status of management action. This follow-up may take the form of a discussion or perhaps a limited review. Audit R2011-14 will remain open until we have evaluated the actions taken.

We appreciate the cooperation and assistance provided by you, as well as your and other departments' staff. Should you have any questions concerning the report, please do not hesitate to contact me.

Michael R. Jenson
Director

xc: Audit Committee Members
Chief Financial and Administrative Officer, Gupta

UNIVERSITY OF CALIFORNIA AT RIVERSIDE

AUDIT & ADVISORY SERVICES

MEMBER OF ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

INTERNAL AUDIT REPORT R2011-14

SYSTEMWIDE AUDIT – ELECTRONIC INFORMATION SECURITY – BFB IS-3

JUNE 2011

Noahn Montemayor
Principal Auditor

Laura Bishin
Principal Auditor

Approved by:

Michael R. Jenson
Director

UC RIVERSIDE
SYSTEMWIDE AUDIT – ELECTRONIC INFORMATION SECURITY – BFB IS-3
INTERNAL AUDIT REPORT R2011-14
JUNE 2011

I. EXECUTIVE SUMMARY

Based upon the results of work performed within the scope of the audit, it is our opinion that the UC Riverside, with the exception of the issues noted in the Observations (Section VIII), is generally in compliance with Business and Finance Bulletin IS-3 *Electronic Information Security*.

Campus management has taken a proactive approach and made progress in enhancing controls as evidenced by the following positive observations:

1) Computing & Communications (C&C) has taken positive actions to resolve previous audit observations and has responded well to recommendations to enhance SAS115 Key IT Controls.

2) C&C has taken an enterprise approach to meet campus electronic information security requirements. Nevertheless, the updated UCR Information Security Plan includes not only efforts, tools, and programs to secure core enterprise systems but also processes, policies, and outreach to assist campus organizational units and departments in ensuring the security of distributed systems and information.

However, we observed one area that needs enhancement to be in compliance with Business and Finance Bulletin IS-3 *Electronic Information Security*.

Confirmation of testing and authorization for moving application programs to production (See Observation at Section VIII).

This item is discussed below. Minor items that were not of a magnitude to warrant inclusion in the report were discussed verbally with management.

II. PURPOSE

UC Riverside Audit & Advisory Services (A&AS), as part of a systemwide audit effort under the direction of the University Auditor's Office, performed an audit to assess compliance with Business and Finance Bulletin IS-3 *Electronic Information Security* on a sample basis, identify areas to improve compliance, and identify recommendations for modifications to the IS-3 policy.

III. BACKGROUND

IS-3 was first published in 1998 with the purpose of establishing guidelines for achieving appropriate protection of University electronic information resources and to identify roles and responsibilities at all levels in the University of California (UC) system. The provisions of IS-3 apply to all University campuses and medical centers, the Office of the President, UC managed national laboratories, and other UC locations (campuses) regarding management of its information assets.

The current version (May 20, 2009) of the IS-3 policy can be found at http://www.ucop.edu/ucophome/policies/bfb/is3.pdf.

In 2007, 2008, and 2009, the University's Chief Information Officers and the information security community undertook a self-assessment of compliance with IS-3 to gauge the strength of information security activities across the system. The self-assessment instrument condensed nearly fifty IS-3 requirements and points of guidance to 17 activity categories for assessment. Each location was asked to provide responses from two distinct perspectives: that of the Central/Campus-wide Information Technology organization and that of the location as a whole but excluding Central/Campus-wide IT (the decentralized view). Medical center responses focused primarily on the central perspective. Responses from the ten campuses, five medical centers, Agriculture and Natural Resources, and UCOP were distilled to come up with the overall assessment of IS-3.

After three years of self-assessment, this review is being conducted by internal audit to provide an independent assessment of IS-3 compliance.

IV. SCOPE

All 10 UC campuses, the UC Office of the President, and Lawrence Berkeley National Laboratory participated in the audit.

The scope of this audit for each location generally included the following IT environments:

1. Central Administrative Computing
2. Distributed Computing Environments for Specific Departments or VC Areas

Medical center and medical group computing are not included in the scope of this audit. IS-3 compliance in these IT environments will be addressed in a future audit.

The potential scope for each IT environment will include the 17 activity categories for assessment (see Table 1) and the respective IS-3 sections III and IV.

Table 1: Assessment Activity Categories

Categories	IS-3 Section(s)
Management Measures: People	
1. Designation of Information Security Officer	III.A. Identification of Information Security Officer (ISO)
2. Security Education & Awareness Training	III.E. Education and Security Awareness Training
Management Measures: Processes	
3. Asset Inventory & Classification	III.B. Risk Assessment, Asset Inventory and Classification
4. Risk Assessment	III.B.1. Risk Assessment
5. Information Security Plan	III.C. Security Plan
6. [Workforce] Administrative	III.C.1. Administrative Workforce Controls
7. Physical/Environmental Controls	III.C.3. Physical and Environmental Controls
8. Incident Response Planning & Notification Procedures	III.D. Incident Response Planning and Notification Procedures
9. Third Party Agreements	III.F. Third-party Agreements
Technical Measures	
10. Identity and Access Management	III.C.2.a. Identity and Access Management
11. Access Controls to Authenticate & Authorize Users	III.C.2.b. Access Controls
12. Systems and Applications Security	III.C.2.c. Systems and Application Security
13. Application Systems Management	III.C.2.c.v. System and applications software development III.C.2.e. Change Management
14. Collection, Management and Analysis of Log Data	III.C.2.f. Audit Logs
15. Data Protection and Encryption	III.C.2.g. Encryption
16. Risk Mitigation Measures	III.C.3.a. Risk Mitigation Measures
17. Network Security Tools & Practices	III.C.2.d. Network Security IV. Minimum Requirements for Network Connectivity

Through the preliminary risk assessment process described in the **Approach** section below, the scope for detailed audit testing for each location was narrowed, (1) to specific IT environments, and further, (2) to specific sections of IS-3 for each IT environment selected.

This audit identifies recommendations for modifications of the IS-3 policy where applicable.

V. APPROACH

Each UC location conducted a preliminary risk assessment to determine:

1. The IT environments to be included in detailed audit testing
2. For each environment selected, the sections of IS-3 in which to perform detailed audit procedures

In conducting the preliminary risk assessment, each location considered using the following sources of information:

- Discussions with selected members of management using the test steps included in section PRELIMINARY SURVEY AND RISK ASSESSMENT in this audit program
- Past Internal Audit Reports on IT Security
- Other recent external/internal reviews of IT functions (i.e., Tiger Team Reports)
- Recent formal IT risk assessments (e.g., annual IS-3 survey)
- Strategic planning documents for IT areas
- Organization charts for central IT areas, and staffing plans
- Action plans developed based on risk assessments, and current status
- Internal vulnerability assessment tools and practices
- Information security plans
- Data inventory and classification schema
- Network diagrams and documentation
- Disaster recovery plan, and disaster recovery test documentation, if available
- Campus Incident Response Team (CIRT) policies and procedures
- Local implementing policy (guidelines, standards, etc.) for IS-3 requirements and minimum network connection standards, if applicable.
- Campus password (complexity) policy

Risk was assessed as *Low*, *Moderate*, and *High* based on the definitions included in the *IS-2 Risk Assessment Matrix – **APPENDIX A***. The risk assessment results are documented in the **Risk Assessment Matrix** at **APPENDIX A**. Detailed audit testing was conducted for *High* risk areas using the steps outlined in the DETAILED TEST PROCEDURES section below. Auditors used their judgment to determine the detailed test procedures as necessary. In cases where specific testing attributes are not met, consideration was given to compensating and mitigating controls that may have been in place before reporting an issue as a potential finding.

Issues identified at the campus/laboratory level have been summarized in a separate audit report for each location. The systemwide Office of Ethics, Compliance and Audit Services will identify common issues reported in local audits which will be summarized in a systemwide audit report.

VI. PRELIMINARY SURVEY AND RISK ASSESSMENT

We conducted and document a risk assessment of IS-3 compliance by category of policy requirements in the 17 major IT areas below. We included key managers from the major IT areas in the formal risk assessment process where appropriate. We were provided a common risk assessment scale and corresponding definitions for the risk assessment process (e.g., low, moderate, and high risk security impacts as noted in IS-2 section III.B.). The Risk Assessment Matrix is documented at **Appendix A**. We selected high risk IT areas for detailed testing, and developed specific test plans for each area selected.

MANAGEMENT MEASURES: PEOPLE

1. Designation of Information Security Officer (IS-3 Section III.A)
   a) Determine designation of Information Security Officer
2. Security Education & Awareness Training (IS-3 Section III.E)
   a) Gain an understanding of employees awareness of System-wide Security Policies
   b) Gain an understanding what Security Awareness training has been offered and attended at the campus

MANAGEMENT MEASURES: PROCESSES

3. Asset Inventory & Classification (IS-3 Section III.B)
   a) Gain a general understanding of the electronic information resources
4. Risk Assessment (IS-3 Section III.B.1)
   a) Gain a general understanding of the primary security objectives for protecting information resources
      - Confidentiality
      - Integrity
      - Availability
   b) Gain a general understanding of the risk in the event of failure that may cause loss of confidentiality, integrity, or availability of information resources
5. Information Security Plan (IS-3 Section III.C)
   a) Gain a general understanding of available security plans
6. [Workforce] Administrative (IS-3 Section III.C.1)
   a) Gain a general understanding of the administrative workforce controls to preserve data integrity and confidentiality
   b) Gain a general understanding of policies and procedures to identify, assign, and revoke access to restricted or essential resources by staff in critical positions
7. Physical/Environmental Controls (IS-3 Section III.C.3)
   a) Gain a general understanding of the established procedures for the physical protection of its resources, particularly resources that support *restricted* or *essential* (as defined in Appendix A of IS-3) systems or data.
   b) Gain a general understanding of the controls for limiting physical access to facilities housing *restricted* or *essential* (as defined in IS-3 Appendix A) resources.

c) Gain a general understanding of the physical security mechanisms in place for equipment vulnerable to unauthorized removal.
d) Gain a general understanding of the procedures in place to track reassignment or movement of devices and stock inventories.
e) Gain a general understanding of the procedures in place for disposition of equipment.
f) Gain a general understanding of the procedures in place to ensure physical security for portable devices and media such as laptop computers, PDAs, memory sticks, CD ROMs, etc.
g) Inquire with management to determine if there have been any physical security compromises in the last year and discuss the results of these incidents.

8. Incident Response Planning & Notification Procedures (IS-3 Section III.D)
   a) Gain an understanding of campus incident response policy and practices, including the following:
      - Local CIRT implementation policy and plan
      - Central and departmental roles and responsibilities
      - Management/committee oversight;
      - Notification procedures, and
      - Forensics capabilities (including tools and techniques)
9. Third Party Agreements (IS-3 Section III.F)
   a) Gain an understanding of purchasing management standards with respect to assuring proper safeguards of University information resources.

TECHNICAL MEASURES

10. Identity and Access Management (IS-3 Section III.C.2.a)
    a) Gain a general understanding of all identity and access management (IAM) strategies and corresponding technologies deployed, including technical measures and controls for authentication and authorization (e.g., Active Directory, Kerberos, RAC-F, Shibboleth, Single Sign on, UC Trust, etc.). Specifically, gain an understanding of the following, if applicable:
       - Access authorization processes, and access rights/roles management
       - Authentication processes, credential requirements (password, phrase, smart-card, token, etc.), and Single Sign-On synchronization
         - Password generation process and complexity requirements
         - Use of shared/generic passwords
11. Access Controls to Authenticate & Authorize Users (IS-3 Section III.C.2.b)
    a) Gain a general understanding of access control strategies and corresponding technologies deployed. Specifically, gain an understanding of the following, if applicable:
       - Measures for session protection, automatic logout
       - Procedures for privileged accounts (super user, root, or administrative access)

- Number of privileged accounts and corresponding job responsibilities
- Logging/monitoring privileged accounts usage
- Termination of privileged accounts

12. Systems and Applications Security (IS-3 Section III.C.2.c)
    a) Gain a general understanding of systems and application security measures including:
        - Personnel assignments for systems administration including separation of duties
        - Security plans
        - Backup and retention processes
        - Measures for protecting against malicious software (viruses, worms, Trojans, etc.)
        - Software development practices and risk/privacy impact assessments
        - Patch management practices
        - Encryption for wireless devices
13. Application Systems Management (IS-3 Sections III.C.2.c.v and 2.e)
    a) Gain a general understanding of software change management practices, version control software in use, and migration practices (from development to quality assurance and to the production environment, if applicable).
14. Collection, Management and Analysis of Log Data (IS-3 Section III.C.2.f)
    a) Gain a general understanding of the audit log management infrastructure, including the extent to which logging has been enabled and logs are reviewed and acted upon when adverse conditions are indicated.
15. Data Protection and Encryption (IS-3 Section III.C.2.g)
    a) Gain a general understanding of the use of encryption for data in transit and data at rest, and encryption key management practices.
16. Risk Mitigation Measures (IS-3 Section III.C.3.a)
    a) Gain a general understanding of appropriate measures for prevention, detection, early warning, and recovery from emergency conditions
17. Network Security Tools & Practices (IS-3 Sections III.C.2.d and IV)
    a) Gain a general understanding of network security strategies and technical security measures (e.g., ACL's, firewalls, IDS/IPS, etc.).
    b) Solicit established policies and standards from responsible IT management to determine if specific standards have been created to address:
        - Access Controls (including Proxy Servers)
        - Password Encryption
        - Patch Management
        - Anti-Virus Protection
        - System management and monitoring (services and ports)
        - Host-Based Firewalls
        - Email Relays
        - Session Timeouts
    c) Assess policies and standards for compliance with IS-3 requirements.

VII. DETAILED TEST PROCEDURES

(As needed per selected high risk locations)

We have identified one (1) high-risk area for testing (APPENDIX A) under Campus Information Services (Central Administrative Computing) - Business and Finance Bulletin IS-3 Electronic Information Security, Section III.C.2.e. - Change Management.

IS-3, Section III.2.C.e components were tested as follows:

1. Verified change management procedures are authorized.
2. Verified steps taken to prevent unauthorized changes. Review to ensure programmers are restricted to specific applications.
3. Examined Change Control Forms (used to track movement of hardware and infrastructure) in Q4 FY10/11 for completeness (i.e. affected service, purpose, impact, risk rank, back out estimate, signoffs, etc.).
4. Verified user training environments and training is available as needed – for significant applications.

Additional components of IS-3, Section III.2.C.e were tested by selecting a judgmental sample of 6 program changes from iScots and 4 program changes selected for self-audit by Computing & Communications and performed the following:

1. Verified that the change management process is planned and supervised.
2. Verified changes are recorded & monitored.
3. Verified changes moved to production were tested by users.
4. Verified changes moved to production were authorized by users and documented in iScots.
5. Verified that IT is performing bi-monthly self audit (2 changes/month) including reviewing audit logs & SourceSafe.
6. Verified back out capabilities (proper use of SourceSafe).

All 10 sample selections were selected from Q4 FY10/11, the period in which updated/enhanced policies were implemented. We selected changes from what we considered to be significant, critical, and sensitive applications (this included systems like Enterprise Access Control System, Banner/Financial Aid, eBuy (Purchasing), ePay (Electronic Payment Request), Facilities Management System, and the new automated timesheet system).

Substantive audit procedures were performed from April through June 2011. Accordingly, this evaluation of internal controls is based on our knowledge as of that time and should be read with that understanding.

VIII. OBSERVATION, RECOMMENDATION, AND MANAGEMENT CORRECTIVE ACTION

Confirmation of Testing and Authorization for moving Application Programs to Production

a) **IS-3, Section III.2.C.3** - Eight of ten program changes selected for testing lacked sufficient documented confirmation of testing and four of ten program changes selected for testing lacked sufficient documented authorization for moving application programs to production.

b) **Local UCR Policy** – Ten of ten program changes selected for testing lacked the application owner's approval to deploy the changes within the Resolution field (of iScots).

COMMMENTS

IS-3, Section III.2.C.e requires that changes to a system (especially restricted or essential resources) be performed according to authorized change management procedures including confirmation of testing and authorization for moving application programs to production.

Also per UCR's local policy 'Computing & Communication's (C&C's) Application Development & Programming Guidelines' – last updated April 2011, page 14, "Enterprise Application Development then notifies the application owner that the software change is complete and available for evaluation and acceptance testing within the TEST environment. If the application owner encounters bugs or other problems during testing, this is communicated to Director of Enterprise Application Development in writing and the Director coordinates with the developer to complete additional work in DEV to rectify the problem. Once again, the code is applied to TEST and the application owner is notified. This cycle can iterate as many times as necessary until the application owner approves of the changes." And "Ultimately, approval to deploy the changes to PRODUCTION is granted by the application owner and communicated to the Director of Enterprise Application Development in writing. The developer records the application owner's approval to deploy the changes within the Resolution field (of iScots)."

RECOMMENDATION – C&C

a) **IS-3, Section III.2.C.3** - We recommend that confirmation of testing and authorization for moving application programs to production be properly documented and retained in order to comply with IS-3, Section III.2.C.e.

b) **Local UCR Policy** – We further recommend that owner approval be included within the Resolution field of iScots as per UCR local policy.

MANAGEMENT RESPONSE – C&C

Computing and Communications (C&C) requires that all new software, program enhancements, and trouble remediation be tested and subsequently receive business / functional approval prior to migration to the production environment (with the exception of serious problems that are severely impacting operations). For the various code changes that were reviewed by Audit and Advisory Services, such testing occurred and approval was obtained, but it was not explicitly recorded within C&C's change control system (iScots). Per the audit recommendation noted above, C&C will ensure that future testing efforts and business / functional migration approvals are explicitly recorded (e.g. approval e-mails will be copied to the change control system, etc.).

RECOMMENDATION – OFFICE OF THE PRESIDENT

We also recommend that the UC Office of the President consider clarifying IS-3, Section III.2.C.e to indicate who should perform and confirm testing (e.g. users and/or programmers), and who should provide authorization for moving application programs to production.

UC RIVERSIDE
R2011-14 Electronic Information Security - BFB IS-3
Preliminary Risk Assessment

SOURCE: Matt Hicks, Audit Manager-Systemwide, OP

PURPOSE: Conduct and document a risk assessment of IS-3 compliance by category of policy requirements in the major IT areas. Use form below. Using common risk assessment scale and corresponding definitions for the risk level (i.e., Low, Moderate, or High), assess both the LIKELIHOOD that the risk that failure to achieve a particular security objective will occur and the IMPACT on UCR should the failure to achieve the security objective occur. Select high risk IT areas for detailed testing, and develop specific test plans for each area selected. Through the preliminary risk assessment process, the scope for detailed audit testing for each location should be narrowed, (1) to specific IT environments, and further, (2) to specific sections of IS-3 for each IT environment selected. The systems chosen will be those that are essential for the campus and have restricted data.

CONCLUSION: Based on preliminary risk assessment, we identify one (1) high-risk area for review: Campus Information Services (Central Administrative Computing) Application/Systems development change management policies and procedures, including segregation of duties, documentation, and management control practices.

Assessment Categories	IS-3 Table of Contents (Requirements)	Campus Information Services	Distributed Computing Environments (Depts/VC Areas)				
			Chancellor, EVC & Provost	Finance & Business Ops	Research	Student Affairs	University Advancement
Management Measures: People							
1. Designation of Information Security Officer	III.A. Identification of Information Security Officer (ISO)	M	L	L	L	L	L
2. Security Education & Awareness Training	III.E. Education and Security Awareness Training	M	L	L	L	L	L
Management Measures: Processes							
3. Asset Inventory & Classification	III.B. Risk Assessment, Asset Inventory and Classification	M	L	M	L	M	L
4. Risk Assessment	III.B.1. Risk Assessment	M	M	M	M	M	M
5. Information Security Plan	III.C. Security Plan	M	M	M	M	M	M
6. [Workforce] Administrative	III.C.1. Administrative Workforce Controls	M	L	L	L	L	L
7. Physical/Environmental Controls	III.C.3. Physical and Environmental Controls	M	M	M	M	M	M
8. Incident Response Planning & Notification Procedures	III.D. Incident Response Planning and Notification Procedures	M	L	L	L	L	L
9. Third Party Agreements	III.F. Third-party Agreements	M	L	L	L	L	L
Technical Measures							
10. Identity and Access Management	III.C.2.a. Identity and Access Management	M	M	M	M	M	M
11. Access Controls to Authenticate & Authorize Users	III.C.2.b. Access Controls	M	M	M	M	M	M
12. Systems and Applications Security	III.C.2.c. Systems and Application Security	M	M	M	M	M	M
13. Application Systems Management	III.C.2.c.v. System and applications software development	M	L	L	L	L	L
	III.C.2.e. Change Management	L	L	L	L	L	L
14. Collection, Management and Analysis of Log Data	III.C.2.f. Audit Logs	M	L	L	L	L	L
15. Data Protection and Encryption	III.C.2.g. Encryption	M	M	M	M	M	M
16. Risk Mitigation Measures	III.C.3.a. Risk Mitigation Measures	M	M	M	M	M	M
17. Network Security Tools & Practices	III.C.2.d. Network Security	M	M	M	M	M	M
	IV. Minimum Requirements for Network Connectivity	L	L	L	L	L	L

RISK ASSESSMENT KEY (IS-2)	Impact of potential harm that failure to achieve any of these security objectives would have on University operations, functions, image or reputation, assets, or the privacy of individual members of the University community.
LOW	The event could be expected to have a limited adverse effect or negative outcome to the University, or result in limited damage to University operations or assets, requiring minor corrective actions or repairs.
MODERATE	The event could be expected to have a significant adverse effect on the University or cause a significant degradation in its mission capability, place the University at a significant disadvantage or result in major damage to University assets, or reputation requiring extensive corrective actions or repairs.
HIGH	The event could be expected to have a severe or catastrophic effect on University operations, assets, or individuals and could be expected to cause a loss of mission capability for a period that poses a threat to human life, results in a loss of major assets, or would result in severe financial impact or impact to the reputation of the University.