December 21, 2011

KAREN MESSER
Director, Biostatistics/Bioinformatics
0901

***Subject:*** ***Cancer Center Data Security – Phase II***
***Audit Project 2012-26B***

The final audit report for Cancer Center Data Security – Phase II, Audit Report 2012-26B, is attached. We would like to thank you and your Information Technology team for the cooperation and assistance we received during the audit.

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. We will contact you at the appropriate time to evaluate the status of the corrective actions. At that time, we may need to perform additional audit procedures to validate that actions have been taken prior to closing the audit findings.

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. AMAS also requests that draft reports not be photocopied or otherwise redistributed.

Stephanie Burke
Assistant Vice Chancellor
Audit & Management Advisory Services

Attachment

cc: E. Babakanian
D. Brenner
T. Chen
I. Goodman
C. Klock
R. Lee
T. McAfee
G. Matthews
V. Nandigam
T. Perez
S. Vacca
K. Wottge

# AUDIT & MANAGEMENT ADVISORY SERVICES


## Cancer Center Data Security – Phase II
## Biostatistics/Bioinformatics
## December 2011

**Performed By:**

Daren Kinser, Auditor
Jennifer McDonald, Auditor
Terri Buchanan, Manager

**Approved By:**

Stephanie Burke, Assistant Vice Chancellor

Project Number: 2012-26B

## Table of Contents

## I. Background

Audit & Management Advisory Services (AMAS) has completed a review of the data security processes and technologies implemented by Biostatistics/Bioinformatics (BI) to manage the network that supports its Moores Cancer Center operations. This report provides the results of our review.

The Moores Cancer Center (MCC) is one of five UCSD School of Medicine (SOM) Organized Research Units (ORUs). Established in 1979, the MCC is one of 40 National Cancer Institute (NCI) designated Comprehensive Cancer Centers in the United States. MCC research laboratories and clinic facilities support clinical and non-clinical cancer related research projects, cancer prevention and outreach programs, and comprehensive clinical care.

BI is a MCC shared resource that provides consultation and collaboration services in study design and data collection and analysis to MCC Principal Investigators (PI) who have a shared focus on translational cancer research. BI helps to achieve advances in large scale data analysis, probabilistic methods, high-performance computing, and informatics architecture for cancer research by providing services for:

- Data analysis and interpretation for MCC research projects using contemporary statistical and bioinformatics' methodologies;
- Development and support of electronic data capture systems for investigator-initiated therapeutic clinical trials, observational studies, patient registries and other needs;
- Statistical/Bioinformatics expertise in study design, including research proposal development, sample size determination and power calculation, and analysis plans
- Development of study-specific databases to support MCC research and develop and maintain these databases in a uniform manner;
- Methodological research in cancer-related biostatistics and bioinformatics to support MCC projects;
- Provide education in biostatistics and bioinformatics to graduate students, oncology residents, fellows and MCC investigators; and
- Discussion of miscellaneous statistical questions of all types.

The BI research network connects to the UCSD campus backbone network, and is managed by an Informatics Lead, a Programmer Analyst, and an Information Security Officer in coordination with campus Administrative Computing and Telecommunications (ACT). The BI Information Technology (IT) team has recently undergone personnel changes with the addition of new staff in March and July 2011. The network consists of eight production servers; three development servers; and three backup and support system servers located at either the San Diego Super Computer (SDSC) or MCC. Much of the data that is processed by and stored on the BI network is highly sensitive personally identifiable information (PII) or protected health information (PHI). Security over this type of information is critical to protect against damage or loss that would

impact BI's ability to provide research computing services, and to ensure compliance with Federal and State laws, and University policies.

Departments that manage sensitive data must be focused on ensuring that network security is adequate to comply with applicable regulations. PII is subject to the provisions of California State Bill 1386. Systems that store PHI are subject to Health Insurance Portability and Accountability Act (HIPAA) privacy and security requirements.

In addition to legislative requirements, BI computer equipment must also conform to University of California (UC) Business and Finance Bulletin IS-3 (IS3), *Electronic Information and Security Policy;* and UCSD Policy and Procedure Manual 135-3 (PPM 135-3), *Network Security*; and PPM 135-3 Exhibit C: *Minimum Network Connection Standards* (Minimum Standards). IS3 establishes guidelines for achieving appropriate protection for University electronic resources and identifying roles and responsibilities at all levels in the University of California system. PPM 153-3 Exhibit C standards provide minimal security requirements for devices that are connected to the UCSD Campus network backbone.

In May 2011, AMAS completed a preliminary network security risk assessment of the BI network based on elements of IS3, PPM 135-3 and the Minimum Standards. The risk assessment results were compiled using information obtained through analyzing responses to a Computer Environment Internal Control Questionnaire (ICQ) and supporting documentation, and conducting follow-up interviews with BI network management personnel. Based on those procedures, we determined that a focused review should be performed for selected areas to verify that certain network security controls were in place and performing as expected.

## II. Audit Objectives, Scope, and Procedures

Based on the preliminary risk assessment performed, the objectives of our review were to determine whether processes and technologies implemented to secure IT resources, and the sensitive data stored on BI system servers were adequate to minimize the risk of unauthorized access or data loss; and to validate that minimum standard security measures implemented were functioning as designed.

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

- Reviewed PPM135-3, Minimum Standards, and IS3;
- Interviewed the BI Director of Shared Resources, and the Information Technology (IT) team to further assess areas of risk;
- Reviewed BI computing policies and standard operating procedures (SOP);

- Analyzed the Access Control Lists (ACL's) that restrict network data traffic to and from BI networked servers;

- Evaluated host-based firewall rules that control incoming and outgoing data traffic to servers;

- Assessed server logs and analyzed activity related to virus protection;

- Reviewed host registration information;

- Performed network vulnerability scanning using Retina on BI servers and evaluated reported vulnerabilities; and,

- Completed an information security review based on elements of IS3, PPM 135-3 and the Minimum Standards (***Attachment A***).

The scope of this review covered BI servers and network components. A detailed web application assessment was performed during a previous ACT review, and was therefore not included within the scope of this audit. In addition, BI client computing devices managed by another IT unit were not evaluated during this review.

## III. Conclusion

Based on our review procedures, we concluded that network security practices appeared generally adequate to ensure the confidentiality, integrity and availability of essential or restricted information system resources and data. However, network vulnerability scans performed during this review identified two areas of risk involving systems and application security on BI servers. In addition, we noted some areas where activities were not in strict compliance with policy requirements including minimum standards; risk assessment activities; information security planning; and security education and awareness training.

Observations and opportunities for improvement are discussed in the remainder of this report.

## IV. Observations and Management Corrective Actions

### A. Systems and Application Security

**Vulnerability scans completed on the BI network identified system and application vulnerabilities on six servers[1], four of which process and manage sensitive information.**

[1] A server is a computer or device on a network that manages network resources.

One of the primary risks to network hardware and data is the potential exploitation of system vulnerabilities[2]. In order to reduce the risk that a vulnerability will be exploited, IS security personnel frequently apply updates and patches to system software and work to ensure proper system configuration. UCSD Minimum Standards include policies related to addressing system vulnerabilities. Section 6.2.3, which is applicable to servers that process sensitive information, requires that software patches be applied within a week of availability. Section 6.4.2.1 requires access to files and computing systems be restricted to authorized clients and users by implementing proper authentication mechanisms.

AMAS completed network vulnerability scans on computing devices administered by BI IT using the Retina Network Security Scanner to identify and rank existing vulnerabilities, and identify ports that were open on system servers. Retina is a proprietary vulnerability assessment tool that identifies known security vulnerabilities by using a current and comprehensive vulnerability database. Credentialed and non-credentialed scans were performed on all active servers. Credentialed scanning allows a detailed view of software patch levels, and high level system configurations. Non-Credentialed scanning provides the same view of the network that is seen by an individual without network permissions. The results of the Retina scans were provided to BI IT personnel under separate cover.

The scans identified two high risk vulnerabilities on two Network Attached Storage (NAS)[3] devices, used to store data backup files. AMAS was advised by BI IT that the data was stored in an encrypted format. However, the configuration parameters for NAS devices allowed unauthenticated communication via a NULL session[4], which could provide information that would be helpful to a person with malicious intent.

In addition, the scans identified medium risk vulnerabilities on four servers, two of which process and manage sensitive information. The vulnerabilities were related to outdated software versions on web servers that could potentially provide information disclosure in the event of an active network exploit.

[2] A system vulnerability is a weakness which allows an attacker to reduce a system's information assurance. A vulnerability reflects the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
[3] A network-attached storage (NAS) device is a server that is dedicated to nothing more than file sharing. NAS devices typically provide access to files using network file sharing protocols.
[4] NULL sessions take advantage of "features" in the Server Message Block (SMB) protocol that exist primarily for trust relationships. NULL connections allow the following information to be obtained from the host (1) list of users and groups (2) list of machines (3) list of shares (4) list of users and host security identifiers.

**Management Corrective Actions:**

1. BI IT advised AMAS that they have remediated the high risk vulnerability noted in the original scans. Follow up vulnerability scans completed on November 23, 2011 did not detect the NULL session vulnerability.

2. BI IT will evaluate the results of the Retina scans and address the medium risk vulnerabilities for sensitive servers that are not deemed to be false positives.

## B. Minimum Standards Compliance

**BI was not in strict compliance with Minimum Standards with regard to vulnerability management and protecting the network against malicious software**.

The UCSD Minimum Standards were implemented to reduce the risk that UCSD computing equipment and data are compromised. Computing equipment configurations or IT management processes that do not meet Minimum Standards represent a significant potential security threat, which could result in substantial mitigation costs if security breaches occur.

1. Vulnerability Management

   ACT IT infrastructure monitors traffic on the network for the purpose of maintaining proper network function. Automated tools are used to proactively scan devices attached to the network to identify vulnerabilities that, if left unaddressed, could allow those devices to be compromised and disrupt network activities.

   Minimum Standards for servers that process and manage sensitive information require that firewall rules allow for comprehensive scanning to be performed by ACT/IT. During the review, we noted that BI employed strict firewall rules on their servers, and recently installed Retina to scan locally for vulnerabilities. However, the firewall rules were not configured to allow comprehensive scanning by ACT, per Minimum Standards requirements. In addition, previous Retina scan reports were not retained to establish a consistent pattern of scanning activity, as required by the department SOP and best practices.

   **Management Corrective Action:**

   BI IT will work with ACT/IT Infrastructure to discuss the best options to allow for vulnerability scanning. In addition, an audit

trail of local scanning activity will be established as required by the BI local scanning policy, which is a best practice.

2. Protect Against Malicious Software

Malicious software, also known as malware, consists of programming code (scripts, active content, and other software) typically used to launch denial of service attacks locally or against other campus systems, and facilitate the sharing of inappropriate data. Malware can be categorized as a virus, worm, adware, spyware, rootkit[5], or Trojan[6]. Anti-virus software is used to prevent, detect, and remove malware, providing a basic level of protection for computing systems.

Minimum Standards for servers that process and manage sensitive information require that anti-virus software be installed and updated on a regular basis. ACT/IT Infrastructure provides free anti-virus software for campus users as well as automated virus definition updates through Academic Computing and Media Services (ACMS) servers. During our review we noted that BI IT had installed the campus provided software. However, log analysis identified one server that processed sensitive information and two additional production servers that were not configured to receive timely virus definition updates from ACMS, which increased the potential of security threats to BI resources.

**Management Corrective Action:**

BI IT has updated the configuration on all three servers to receive timely virus definition updates from ACMS servers.

## C. Risk Assessment

**BI IT would benefit from a comprehensive risk assessment to identify and classify information assets and identify potential risks.**

The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Departments or units that manage information assets and electronic resources should conduct formal risk assessments to determine the level of protection needed to adequately protect various existing information resources, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. As business operations, workflow, or technologies change, periodic reviews should be conducted to analyze these

[5] A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.
[6] A Trojan horse, or Trojan, is software that appears to perform a desirable function for the user prior to run or install, but which, sometimes in addition to the expected function, steals information or harms the system.

changes, to account for new threats and vulnerabilities created by these changes, and to determine the effectiveness of existing controls.

UCOP provides general guidelines for developing a risk assessment, which include:

- Identify assets covered by the assessment
- Categorize potential losses
- Identify threats and vulnerabilities
- Identify existing controls
- Analyze the data
- Determine cost-effective safeguards
- Report to Management

During the review, we noted that BI did not employ a comprehensive risk assessment process. BI IT was able to provide detailed information regarding the systems that they managed; however, specific risks and a level of security necessary to protect those resources were not identified and formally documented.

**Management Corrective Action:**

The BI IT group and BI management will perform a comprehensive risk assessment to identify primary security objectives for protecting information resources. The risk assessment will include classification of the information assets stored on the devices or within the applications and identify the level of security necessary to protect the information resources. Additional Risk Assessment resources are included in ***Attachment B***.

## D. Information Security Plan

**BI IT would benefit from a documented security plan to enhance the security of information assets.**

An information security plan should be developed that takes into consideration the acceptable level of risk for systems and processes. A security plan should account for the management, use, and protection of confidential information; and identify the procedures and controls that are needed to enhance security for information assets. It should also identify cost-effective strategies to be implemented to mitigate the risks that are consistent with organizational goals and business functions. The security plan should be developed at the completion of the risk assessment process. Because BI IT had not performed a comprehensive risk assessment, the security plan to consider acceptable risk levels and proper mitigation was not in place.

**Management Corrective Action:**

BI IT and Management will develop an information security plan that identifies acceptable level of risk for information assets, systems and processes.

## E. Security Education and Awareness Training

**During the review, we noted that BI added several new staff members to their technical team who could benefit from additional introduction to UCSD and UC systemwide information security policies.**

IS 3 provides guidelines for achieving appropriate protection of University electronic information resources and identifies the roles and responsibilities for management of information assets. It describes at a campus level, an Information Security Program be established to contain a comprehensive set of strategies related to technical and non-technical measures, which include guidelines for staff security awareness training and education. UCSD IT training programs typically provide a review of University and campus security policies, guidelines, procedures and standards as well as departmental procedures and best practices that may be implemented to safeguard the campus computing environment.

ACT in conjunction with UCSD Staff Education has developed training programs for persons in technical job classifications responsible for system administration duties in department settings. The goal is to ensure that employees responsible for maintaining the UCSD computing environment receive the tools and information they need in order to safeguard sensitive systems and information. During the review, we noted that BI IT was in the process of restructuring its IT organization and adding new members to the IT team. As a result, some IT personnel were not completely familiar with the requirements of campus Minimum Standards and IS3. Additional training would help to ensure that BI systems are maintained in accordance with policy requirements.

**Management Corrective Action:**

BI IT will attend the reinstated UCSD Staff Education IT training series, as it is available, to obtain additional exposure to campus and UC systemwide policy awareness and implementation.

***Cancer Center Data Security – Phase II***
***Biostatistics/Bioinformatics***
***Audit & Management Advisory Services Project 2012-26B***
***Information Security Review Matrix - Attachment A***

| Assessment Categories | Objective | Observations |
|---|---|---|
| **Technical Measures** | | |
| 1. Identity and Access Management | Assess the technical measures for controlling authentication and authorization (password policy, access rights/roles). | No Reportable Observations |
| 2. Access Controls to Authenticate and Authorize Users | Assess the controls for session protection, automatic logout, and procedures for managing privileged accounts. | No Reportable Observations |
| 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. | **See Report Observation A** |
| 4. 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. | No Reportable Observations |
| 5. Collection, Management and Analysis of Log Data | Assess the audit log infrastructure and review practices. | No Reportable Observations |
| 6. Data Protection and Encryption | Assess the use of encryption for data in transit and data at rest. | No Reportable Observations |
| 7. Risk Mitigation Measures | Assess the process for prevention, detection, and recovery from emergency conditions. | No Reportable Observations |
| 8. Network Security Tools and Practices | Assess the network security strategies and technical security measures (Minimum Standards for Network Connectivity). | **See Report Observation B** |

| Assessment Categories | Objective | Risk Assessment |
|---|---|---|
| **Management Measures: Processes** | | |
| 9. Asset Inventory and Classification | Assess the process for identifying electronic information resources. | No Reportable Observations |
| 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 | **See Report Observation C** |
| 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. | **See Report Observation D** |
| 12. Workforce Administration | Assess the protection for granting and/or revoking authorizing and protecting access to information systems. | No Reportable Observations |
| 13. Physical/Environmental Controls | Assess the procedures for physical protection of resources that support restricted or essential systems and/or data. | No Reportable Observations |
| 14. Incident Response Planning and Notification Procedures | Assess the process for reporting and handling a security incident | No Reportable Observations |
| **Management Measures: People** | | |
| 15. Security Education and Awareness Training | Assess employee's awareness of System-wide Security policies. | **See Report Observation E** |

## Risk Assessment Methodology Overview [1]

Many different approaches to risk assessment have been developed. These following guidelines provide a simple step-by-step process. Additional resources and methodologies are linked under Resources to help you establish an approach appropriate to your business environment.

## General Guidelines for a Risk Assessment

1. **Establish the risk assessment team**. The risk assessment team will be responsible for the collection, analysis, and reporting of the assessment results to management. It is important that all aspects of the activity work flow be represented on the team, including human resources, administrative processes, automated systems, and physical security.
2. **Set the scope of the project.** The assessment team should identify at the outset the objective of the assessment project, department, or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed, and operations to be observed.
3. **Identify assets covered by the assessment**. Assets may include, but are not limited to, personnel, hardware, software, data (including classification of sensitivity and criticality), facilities, and current controls that safeguard those assets. It is key to identify all assets associated with the assessment project determined in the scope.
4. **Categorize potential losses**. Identify the losses that could result from any type of damage to an asset. Losses may result from physical damage, denial of service, modification, unauthorized access, or disclosure. Losses may be intangible, such as the loss of the organizations' credibility.
5. **Identify threats and vulnerabilities**. A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Include natural threats, accidental threats, human accidental threats, and human malicious threats. These could include power failure, biological contamination or hazardous chemical spills, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism. A vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc.
6. **Identify existing controls**. Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.
7. **Analyze the data**. In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to analyze data includes preparing a list of assets and showing corresponding threats, type of loss, and

[1] Risk Assessment Methodology gathered from UCOP website

vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

8. **Determine cost-effective safeguards**. Include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle of the safeguard.
9. **Report**. The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read, and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your organization. The report should include findings; a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

**Additional Resources:**

Departmental Security Review and Planning

http://www.ucop.edu/irc/itsec/securityreview.html

BFB IS-2 Inventory, Classification, and Release of University Electronic Information

http://www.ucop.edu/ucophome/policies/bfb/is2.pdf

Risk Assessment Resources

http://www.ucop.edu/irc/itsec/riskresources.html