

IT Security Policy Compliance Auditing

**UC First Annual Compliance and Audit Symposium
February 2009**

Greg Loge, Manager of IT Audit
UC Davis

Introduction

Greg Loge, M.B.A., CISSP, GIAC GSNA

Manager of IT Audit

University of California Davis

ggloge@ucdavis.edu

Agenda

- Overview of the UC Davis “Cyber-Safety” IT Security Policy PPM 310-22
- Minimum Security Standards – PPM 310-22 Exhibit A
- IT Audit Program

Policy

- Policy and Procedure Manual (PPM) 310-22, Cyber-Safety Policy, was established in April of 2005 to address the need for minimum security standards for IT resources at UC Davis.
- The policy consists of 16 standards for computing devices connected to the campus network, an annual compliance reporting and planning process for campus units, and an exception process for requesting exceptions to policy.

PPM 310-22

- UC Davis security standards ([Exhibit A](#)) will be published and maintained by Information and Educational Technology (IET). The standards will be reviewed annually by senior campus administrators and technical representatives.
- Campus units must ensure devices connected to the campus network comply with the security standards or develop/implement strategies to mitigate the risks posed by non-compliance.

PPM 310-22

- Campus units must annually report to their respective Dean, Vice Chancellor or Vice Provost, the extent to which unit operations are consistent with the campus security standards.
- Where compliance is not complete, the report must document a compliance plan, a statement indicating a specific security standard is not applicable or an acknowledgement and acceptance of the information risks associated with continued non-compliance to the security standard.

PPM 310-22

- These reports will be summarized by the Deans, Vice Chancellors and Vice Provosts and submitted annually, starting no later than July 1, 2006, to the Offices of the Chancellor and Provost. The reports will be used to prepare a campus-wide annual report describing the state of UC Davis computing and network security.

Annual Reporting

- 21 Reporting units representing the main administrative areas on the UC Davis Campus:

College of Agricultural and Environmental Sciences

College of Biological Sciences

College of Engineering

College of Letters and Science – Humanities, Arts and Cultural Studies

College of Letters and Science – Mathematical and Physical Sciences

College of Letters and Science – Social Sciences

Graduate School of Management

Information and Educational Technology

Office of Administration

Offices of the Chancellor and Provost

Office of Graduate Studies

Office of Research

Office of Resource Management and Planning

Office of Student Affairs

School of Education

School of Law

School of Veterinary Medicine

UC Davis Health System

University Extension

University Library

University Relations

Exhibit A - Standards

- 16 Minimum Security Standards all devices attached to the UC Davis network must meet, or have appropriate additional controls in place to mitigate the risk of non-compliance
- Exceptions:
 - “Campus Administrative Officials” may approve exceptions for certain systems compliance with a Exhibit A standard.

Exhibit A - Standards

- Divided into two priority levels.
 - Level I practices (Highest Priority)
 - Software Patch Updates
 - Anti-virus Software
 - Nonsecure network services
 - Authentication
 - Personal Information
 - Firewall Services

Exhibit A - Standards

- Divided into two priority levels.
 - Level II practices (Secondary Priority)
 - Physical Security
 - No Open Mail Relays
 - Proxy Services
 - Audit Logs
 - Backup and Recovery
 - Training for Users, Administrators, and Managers
 - Anti-Spyware Software
 - Release of Equipment with Electronic Storage
 - Incident Response Plan
 - Web Application Security

Exhibit A - Standards

- What standards should be audited?
 - Focus on the Level I high priority standards first.
 - Include level II standards as appropriate:
 - Web Application Security when web applications are identified that deal with Personally Identifiable Information (PII)
 - Disaster Recovery – important area and one of common weakness found across almost all departments
 - Consider narrowing focus further for very large, centralized, enterprises, and approach auditing various standards as separate projects.
 - Health System

Exhibit A - Standards

- Software Patch Updates:
 - Computers connected to the campus network must use an operating system and application software for which the publisher maintains a program to release critical security updates. Campus units must apply all currently available critical security updates within seven calendar days of update release or implement a measure to mitigate the related security vulnerability. Exceptions may be appropriate for specialized and/or research operating systems, patches that compromise the usability of an operating system or application or for patches for which the installation is prohibited by regulation.

Exhibit A - Standards

- Anti-virus Software:
 - Anti-virus software must be running and updates must be applied within no more than 24 hours of update release for computing hosts connected to the campus network. This standard applies to computers and PDAs connected to the campus network using Windows, Mac OS X, Linux, Palm, or Windows Mobile PC operating systems.

Exhibit A - Standards

- Nonsecure Network Services:
 - Computers connected to the network must use only network services/processes that are needed for their intended purpose or operation. All unnecessary services must be disabled. Where such services are operationally required, the available encrypted equivalent service must be used (e.g., SSH rather than Telnet) if data of a restricted nature, such as passwords or other confidential information, will be transmitted by the service. This standard applies to computers using the Windows, Mac OS X, or Linux operating systems.

Exhibit A - Standards

- Authentication:
 - Campus electronic communications service providers must have a suitable process for authenticating users of shared electronic communications resources under their control.
 - 1. No campus electronic communications service user account shall exist without passwords or other secure authentication system, e.g. biometrics, Smart Cards.
 - 2. Where passwords are used to authenticate users, the password selection method must be configured to prohibit the use of passwords found in common dictionaries or that match the account name.
 - 3. All default account passwords for network-accessible devices must be modified upon initial use.
 - 4. Passwords used for privileged accounts must not be the same as those used for non-privileged accounts.
 - 5. All campus devices must use encrypted authentication mechanisms unless an exception has been approved by a senior administrative official. Unencrypted authentication mechanisms are only as secure as the network upon which they are used. Any network traffic may be surreptitiously monitored, rendering unencrypted authentication mechanisms vulnerable to compromise.
-

Exhibit A - Standards

- **Personal Information:**
- Campus units must identify departmental computing systems and applications that house personal information (personal name along with Social Security number, California driver identification number, financial account information, health insurance information, or medical account information). Personal information must be removed from all computers for which it is not required. If the personal information cannot be removed from the computing system, the campus unit must develop a plan specifically outlining how the information and systems will be kept secure. Measures to protect the information could include removing several digits from the personal identifiers, moving the files to removable media and storing this media in a secure location apart from the computer, or encrypting the personal information.

Exhibit A - Standards

- **Personal Information:**
- Campus units providing electronic personal information as defined above, to any private party must do so by formal agreement. The agreement must include a provision that the party receiving the electronic personal information will abide by these data standards. A formal agreement is not necessary with governmental agencies that receive electronic personal information. However, campus units are encouraged to discuss the privacy and security requirements pertaining to the shared data with these agencies to ensure similar standards of compliance.
- Campus units that develop network-based applications that host personal information must use secure application coding practices (***See web application security standard coming up***)

Exhibit A - Standards

- **Firewall Services:**
- Campus units must deploy and maintain both a network (VLAN) firewall and host-based firewall service for network connected computers. The firewall must contain ingress rules that are restrictively configured to deny all traffic unless expressly permitted. Egress firewall rules must be configured to deny identified malicious network traffic if not configured to deny all traffic unless expressly permitted.

Exhibit A - Standards

- ****Web Application Security:**
- Web applications developed or acquired by campus units must support secure coding practices. Web applications must mitigate the vulnerabilities described within the OWASP Top Ten Critical Web Application Security Vulnerabilities.

Exhibit A - Standards

- ****Backup and Recovery:**
- Campus units must develop, implement, and maintain a backup plan for restricted information residing on electronic storage. The backup media must be protected from unauthorized access and stored in a location that is separate from the originating source. The backups must be tested on a regular basis to ensure recoverability from the backup media.

Audit Objectives

- Review recent submitted cyber-safety reports for:
 - Completeness:
 - Accuracy:
- Review exception reporting process
- Review level and adequacy of compliance planning present to address identified areas of non-compliance
- Conducted detailed testing of compliance with our in scope security standards

Audit Objectives

- Review recent submitted cyber-safety reports for:
 - Completeness:
 - Have all departments within the reporting unit been included in the report?
 - Accuracy:
 - Do the submitted reports accurately represent the level of compliance to the Exhibit A Standards that are within scope of our audit?

Audit Objectives

- Review approved exceptions to policy:
 - How are exception requests documented?
 - Who approved the request? (must be a “Senior Manager or designee”)
 - Are there controls in place to mitigate the risk of non-compliance?
 - Are they adequate?

Audit Objectives

- Review level and adequacy of compliance planning present to address identified areas of non-compliance:
 - Are there plans in place to address reported areas of non-compliance, that do not have an exception to policy approved by senior management?
 - Are the plans adequate?
 - Are there details of how compliance will be achieved?
 - Timelines/milestones/deadlines?
 - Assigned responsible parties?

Audit Objectives

- Conducted detailed testing of compliance with our in scope security standards
 - Sampling of systems/units to be tested in detail
 - Testing tools and methods (more on this later)

Audit Methodology

- Selection of reporting Dean/VC/VP area for review (one of the 21 units listed previously).
 - Risk Based
 - Factors to consider:
 - Business/mission
 - Submitted cyber-safety reports
 - Known stores of PII
 - Recent security incidents

Audit Methodology

- Dean/VC/VP Area:
 - Review completeness of recent cyber-safety report submitted
 - Review exception reporting and approval process (if any exceptions have been requested/reviewed)
 - Review compliance plans
 - Identify high risk applications, business units, or departments within the Dean/VC/VP area for detailed Exhibit A compliance testing.
 - Conduct detailed Exhibit A standard review for standards within scope for systems within the Dean/VC/VP office
 - Almost always this unit will be one of the selected units for detailed testing due to the nature of their business
-

Audit Methodology

- Sampling of departments in Dean/VC/VP area to conduct detailed Exhibit A standard compliance testing
 - Risk based:
 - Interviews with senior managers in the Dean/VC office under review
 - Business/mission
 - Cyber-safety reports
 - Known stores of PII

Audit Methodology

- Detailed review of in scope Exhibit A standard compliance:
 - Testing of sampled department's systems for compliance with the standards that are in scope.
 - May require further sampling to reach a manageable number of systems for review.
 - Servers
 - Representative end user systems
 - » Sample of faculty labs
 - » Administrative office systems

Exhibit A Standard Testing

- Level I practices
 - Software Patch Updates - Nessus
 - Anti-virus Software - Nessus
 - Nonsecure network services - Nessus
 - Authentication – Nessus
 - Personal Information – Identity Finder
 - Firewall Services – Nessus/Nmap
- Level II practices
 - Web application security – IBM AppScan Enterprise
 - Disaster recovery – Documentation Review, Interviews/demonstration

Exhibit A Standard Testing

- Level I practices
 - Software Patch Updates - Nessus
 - Anti-virus Software - Nessus
 - Nonsecure network services - Nessus
 - Authentication – Nessus
 - Personal Information – Identity Finder
 - Firewall Services – Nessus/Nmap
- Level II practices
 - Web application security – IBM AppScan Enterprise
 - Disaster recovery – Documentation Review, Interviews/demonstration

Network/Vulnerability Scanning

- Goal: Ensure a repeatable, reliable, and thorough means for validating the security of sampled systems.
- Advantages:
 - Ability to interrogate a large number of systems efficiently.
 - Identification of systems attached to the network that may not be known or disclosed by IT staff initially through interviews.
 - Broad number of systems and security issues can be evaluated
 - Windows
 - Unix
 - Macs
 - Identification of rogue wireless access points
 - Identification of suspicious or possibly compromised systems
 - Wide range of client software supported
 - Adobe Flash, Acrobat
 - Java
 - Browsers (Firefox, IE)

Network/Vulnerability Scanning

- Caveats:
 - Scanning can be **DANGEROUS!**
 - Various tests can crash a system
 - Some tests are designed to attempt to crash a system
 - DOS plugins
 - Use “safe checks”
 - Degraded performance on production systems
 - Get approval from the highest authority possible *in writing*.
 - Scan only with proper notification/planning with client*

Network/Vulnerability Scanning

- Caveats:
 - Authenticated scans are necessary for full testing:
 - Issuing of temporary credentials with local admin rights on systems to be tested.
 - Allow administrative access over the network – Active Directory GPO.
 - Host based firewalls will limit scanner's ability to evaluate the system.
 - Assign specific IP to scanner.
 - Create exceptions in firewall for scanner. – Active Directory GPO
-

Network/Vulnerability Scanning

- Caveats:
 - Consider network topology
 - Network firewalls between scanner and systems being evaluated?
 - IPS?
 - Be available during scan for clients to contact you if issues arise.

Audit Reports

- Background
- Process
- Executive Summary
- Executive Summary Table
- Findings tables by standard reviewed
- Appendix or especially detailed data can be in a separate confidential document shared with IT staff.

Audit Reports

- Findings can be extremely sensitive
 - Leave specific details out of final report when possible
 - “Patches are not applied within 7 days per policy” versus “All systems are running Java RTE 1.4”
 - Specifics can be shared as a separate confidentially marked work paper (e.g., Nessus reports)
 - Entire audit report may need to be marked and treated confidential

Executive Summary

IAS identified significant areas of risk to XXXX operations resulting from deficiencies in compliance to PPM 310-22 security standards. The deficiencies increase the risk of loss of operational data, theft of personal information and disruption to critical business processes. Two of the seven Cyber-Safety areas were reported accurately, however the remaining five areas had many deficiencies which are not accurately identified in the FY 07-08 cyber-safety report. These deficiencies and inaccurate reports raise concerns that risks are not adequately communicated to management to be appropriately addressed.

Executive Summary

Areas Reviewed	Results	Accurately reported in FY 06-07?	Risk
Compliance Planning	•Insufficient	Not Applicable	Medium
Exception Reporting	•None requested	Not Applicable	Not Applicable
Software Patch Updates	•Partially Compliant	No	Medium
Antivirus	•Partially Compliant	No	Medium
Non-secure Network Services	•Not Compliant	Yes	Medium
Authentication	•Partially Compliant	No	Medium
Personal Information	•Partially Compliant	No	High
Firewall Services	•Not Compliant	Yes	High
Disaster Recovery	•Not Compliant	No	High

General Cyber-Safety Observations

- Several areas of the cyber-safety report for FY 07-08 were not accurately reported
- Compliance plans do not address all areas of noncompliance
- No exceptions were requested for areas of noncompliance

Software Patch Updates

Observations	Accurately reported in FY 06-07?	Management Corrective Action	Priority
Critical Security Patches are not applied within 7 days of release.	No	Develop and implement a procedure for testing and applying critical security patches within 7 days of release for all software on XXXXX systems. Action Date: 1/1/2009	Medium
Several software packages were identified that are no longer supported by the manufacturer, thus are unable to receive critical security updates.	No	Inventory all software installed on XXXXX systems and remove applications no longer supported by the manufacturer. Action Date: 1/1/2009	Medium

Antivirus Software

Observations	Accurately reported in FY 06-07?	Management Corrective Action	Priority
Effective procedures are not in place to ensure all systems are running up to date antivirus. Several systems were observed not running an up to date Antivirus client.	No	Install supported antivirus software on all XXXXX systems and configure it to update every 24 hours. Action Date: 1/1/2009	Medium

Questions?

Greg Loge, M.B.A., CISSP, GIAC GSNA

Manager of IT Audit

University of California Davis

ggloge@ucdavis.edu