****

**Security Plan Audit Report**

**on**

**Pacific College of Oriental Medicine**

**Submitted by**

Christian Larsen, CISSP, CISM

Harshal Sanap

Ilya Shuster

Jeremy Silverstein, CISSP, CEH

Alessandro Vomero

**MIS 755: Information System Security Management**

**June 30, 2018**

Contents

[1 Organization Overview 3](#_Toc518123124)

[1.1 What They Do 3](#_Toc518123125)

[1.2 Where they are / location information 3](#_Toc518123126)

[1.3 Data / information they have and how they use it 3](#_Toc518123127)

[1.4 Size / key personnel 3](#_Toc518123128)

[2 Audit Methodology 4](#_Toc518123129)

[3 Audit Results 5](#_Toc518123130)

[3.1 Top Five Positive Findings 5](#_Toc518123131)

[3.1.1 Knowledge and security consciousness of IT staff 5](#_Toc518123132)

[3.1.2 The use of Amazon Web Services (AWS) 5](#_Toc518123133)

[3.1.3 Information Systems Security Plan (ISSP) in development 5](#_Toc518123134)

[3.1.4 Strong firewall configuration 5](#_Toc518123135)

[3.1.5 Effective use of VLANs 6](#_Toc518123136)

[3.2 Other Positive Findings 6](#_Toc518123137)

[3.3 Top 5 Negative Findings 6](#_Toc518123138)

[3.3.1 No documentation of internal audits or risk assessments 6](#_Toc518123139)

[3.3.2 The ISSP is not up to date or approved 6](#_Toc518123140)

[3.3.3 No documented implementation plan for needed updates 6](#_Toc518123141)

[3.3.4 No documented Configuration Management (CM) program 6](#_Toc518123142)

[3.3.5 No documented Vulnerability Management (VM) program 7](#_Toc518123143)

[3.4 Other Negative Findings 7](#_Toc518123144)

[4 Recommendations 7](#_Toc518123145)

[4.1 Conduct Full Security Audit/Risk Assessment 7](#_Toc518123146)

[**4.2** Update Information System Security Plan (ISSP) 8](#_Toc518123147)

[4.3 Create Plan of Action and Milestones (POA&M) 8](#_Toc518123148)

[4.4 Implement Server Security Standards 8](#_Toc518123149)

[4.5 Implement Automated Vulnerability Scanning 9](#_Toc518123150)

[5 Conclusions 9](#_Toc518123151)

[5.1 Overall risk level 9](#_Toc518123152)

[5.2 Plan / roadmap to get better 9](#_Toc518123153)

[6 Appendix A - Other Recommendations 10](#_Toc518123154)

[7 Appendix B - Sample POA&M 11](#_Toc518123155)

# Organization Overview

## What They Do

Pacific College of Oriental Medicine was founded in 1986 to provide Oriental medical and Asian bodywork therapy education to students from around the world. Since its inception, the College has been at the forefront of educating students and working in conjunction with lawmakers and medical professionals to advance the standards of both the holistic medicine profession and the College's curriculum.

Pacific College has received awards for its acupuncture and Oriental medicine curriculum and clinical training, as well as research grants from the National Institutes of Health and Patient-Centered Outcomes Research Institute, among others. Their alumni have gone on to be successful in the field and are currently sought after as both teachers and practitioners in the U.S. and abroad today.

## Where they are / location information

Pacific College of Oriental Medicine consists of three physical campuses:

* Pacific College San Diego - located at 7445 Mission Valley Rd, Suites 105, San Diego, CA 92108.

**Note**: for the purposes of this audit, we focused only on the San Diego location and the company’s Amazon Web Services hosting environment.

* Pacific College Chicago - located at 65 East Wacker Place, 17th & 21st floor, Chicago, IL 60601.
* Pacific College New York - located at 110 William Street, 19th Floor, New York, NY 10038.

In addition to the physical campuses Pacific College also offers online programs.

## Data / information they have and how they use it

The Pacific College network infrastructure consists of an interconnected network throughout the various campuses. The network connects workstations to network files system, printers, hosts applications and connects to the internet, as well as manages user logins and permissions.

The network attached storage (NAS) device holds data utilized by staff in everyday operations and holds files backup; it is located at the San Diego campus. Cloud-based Office 365 Enterprise A1 provides email services, OneDrive cloud data storage and SharePoint - a web-based portal, for employees, faculty and students.

## Size / key personnel

Pacific College has about 105 employees in their administrative staff, 200 employees in their academic staff. The IT staff consists of 6 people. Their key personnel on the administrative side are the following:

Alexander Diaz, ITT

Gregory Russo, ITT

Gregory A. Talavera, MD MPH - SBLRC, Director

Ana C. Talavera HCHS/SOL Project Director

Paulina Martinez-Mendoza, SBLRC Project Manager

Johanne B. Hernandez, HCHS/SOL Clinic Operations Manager

Ana Rebeca Alvarez-Malo, HCHS/SOL Clinic Operations Coordinator

Tasi Rodriguez, SBLRC Project Manager

# Audit Methodology

For the security audit project we selected Pacific College of Oriental Medicine as our client with the help of Professor Jennex. We started creating an audit plan by gathering the requirements from Alexander Diaz who is a security professional with the pacific college. Our audit plan was limited to the San Diego division of the organization with focus only for the overall security, server and physical security aspect. For each of these sections, we drafted multiple questions which would give us a good viewpoint of the company’s current security standpoint.

For conducting the audit, we used the following regulations:

* FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
* NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations
* NIST SP 800-171 Protecting Controlled Unclassified Information in NonFederal Information Systems and Organizations
* NIST Cybersecurity Framework Version 1.1
* Gramm-Leach-Bliley Act (GLBA)

The draft of audit plan was created by abiding to above regulations and the requirements mentioned by Alex. It was later approved by Prof. Jennex and Alex. The audit plan included the purpose, scope, procedure and the expected outcome as well as a section for the findings of the audit. We received an appointment on June 27 to conduct our audit and interview Alex between 1pm – 5pm. The audit methodology is described section wise below:

**Overall Security Plan:**

For this we first checked if the organization has an ISSP based on the applicable standards and we also checked if that ISSP is actually being approved by some defined personnel of the organization. The organization was further assessed to check if they have a documented process for regular review and update of the ISSP. They were also assessed to check if they maintain a policy for managing the user accounts. Lastly for this section we checked if the organization adheres to the policy outlined in the ISSP for the use of flash drives at workstations. For this we ran a small experiment where we told the organization to use our flash drives to access the audit plan with the intention to see if the USB will be accessible or not on their computer.

**Server Security plan:**

The organization was assessed to check if they maintain a document for vulnerability management that identifies and resolves the vulnerabilities found on the servers in a timely manner. We also checked if they maintain a policy that states the requirements for complexity and aging of the passwords. We also assessed the organization by checking if there is an inventory of devices that is accurate and up to date. We also checked how the sensitive data at rest is stored on the AWS servers whether it is in encrypted format or not. Lastly, we assessed if the organization have configured all the servers according to the company approved baselines while maintaining documentation of all the changes in configuration management program.

**Physical Security plan:**

We checked if the organization monitors all the accesses to the server room by using a security log book. The organization was also checked for having fire protection as well as water flood controls in place for the server room. We also checked if there exists a short-term UPS capability that provides emergency back ups incase of a server shut down. Lastly, the organization was checked for maintaining appropriate temperature and humidity levels within the facility where the information was stored.

The findings of the above mentioned assessment is discussed in the next module.

# Audit Results

## Top Five Positive Findings

### Knowledge and security consciousness of IT staff

The IT staff members that were interviewed by the audit team are responsible for both the system administration and security for the organization’s information systems. They were knowledgeable on applicable standards and industry best practices and were clearly focused on maintaining current security controls and implementing or updating the necessary policies and technology controls.

### The use of Amazon Web Services (AWS)

The organization uses AWS to host nearly all of its 20+ servers. The built-in security features and inherited network security controls greatly enhance the overall security posture and strengthen the availability and disaster recovery process.

### Information Systems Security Plan (ISSP) in development

It was clear that much research and focus has already been dedicated to this effort.  While the ISSP remains under construction, the organization is actively working to determine the correct policies to establish.

### Strong firewall configuration

The organization uses a firewall to monitor all traffic to and from the AWS and local servers.  The firewall has been configured with beneficial features, such as SSL Inspection to allow for the monitoring of encrypted web traffic.  The firewall sends automated alerts to the IT staff when potentially malicious traffic is blocked.

### Effective use of VLANs

Overall, the organization has an effective network security strategy, to include the logical separation of visitor, student, staff, and system administration traffic through the use of VLANs on both its wireless and wired networks.

## Other Positive Findings

* The staff member tested showed an awareness of the threat that could come from a USB storage device.
* The fire extinguisher in the server room complies with the SANS standards (Class-C extinguisher).
* The walls of the server room continue beyond the fake ceiling preventing access to it.
* Strength detector made available to students and staff members during the password creation process.
* Server password is shared between two IT staff members and has minimum strength requirement (8 characters, letters, numbers, special character).
* Use of Paper Cut key fobs to use copy machines.
* Effective backup plan is being used to backup servers to AWS S3 storage.

## Top 5 Negative Findings

### No documentation of internal audits or risk assessments

The organization has not conducted an internal audit or risk assessment.  This is an important first step for the organization to determine its current security posture and prioritize needed improvements and policy implementation.

### The ISSP is not up to date or approved

The ISSP has not been finalized and officially adopted by the organization.  The current draft does not reflect current policies and still requires a substantial amount of work to become an effective document to establish and disseminate policy.

### No documented implementation plan for needed updates

A decision on the exact approach and timeline to implement required policies has not been made. The organization should select a framework that is aligned with NIST SP 800-53, such as the NIST Cybersecurity Framework or the FFIEC Cybersecurity Assessment Tool (CAT).  The IT staff was familiar with these implementation guides, but not actively using one.

### No documented Configuration Management (CM) program

The organization did not have a process to track changes made to its information systems.  An effective CM program should include a review process that considers the security implications of changes made to information systems prior to implementation.  See NIST SP 800-53 CM-1 and NIST SP 800-100 for program requirements. Server baselines should be maintained in accordance with NIST SP 800-53 CM-2.

### No documented Vulnerability Management (VM) program

The site does not conduct vulnerability scans, but does patch systems weekly using the Windows Update feature. Effective vulnerability scanning software will detect much more than the Windows Update feature is able to detect.  Refer to NIST SP 800-53 RA-5 for vulnerability scanning requirements.

## Other Negative Findings

* Doors labeled “Employees only” that were checked by the audit team are unlocked during work hours.
* No humidity control in the server room.
* Double access to the server room: one of the access doors to the server room links to a storage room used by students and could be easily forced open.
* No password policy established (complexity, age, etc not defined).
* No official policy for use of removable media on staff and faculty workstations.
* Device inventory is not up to date.
* No port security on switches; unused switch ports are not disabled.  A potential attacker could gain access to the network by connecting a laptop to the ethernet cable running to a copy machine or by gaining physical access to the switch that resides in a server room which has minimal protection.
* SSL VPN is not configured to only accept TLS connections.  See NIST SP 800-113 (Guide to SSL VPNs) and NIST 800-52 Rev. 1: “This Special Publication provides guidance to the selection and configuration of TLS protocol implementations while making effective use of Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms, and requires that TLS 1.1 configured with FIPS-based cipher suites [be used] as the minimum appropriate secure transport protocol and recommends that agencies develop migration plans to TLS 1.2 by January 1, 2015.”

# Recommendations

## Conduct Full Security Audit/Risk Assessment

Due to the number of findings discovered during our abbreviated security audit, Pacific College should perform an in-depth internal audit in order to ascertain a more complete understanding of their security posture. A full audit will uncover whether they are compliant with their own ISSP as well as industry standards and best practices. The audit will further inform the necessary updates to the ISSP. A full audit will allow for a more complete plan of actions and milestones (POA&M).

The FFIEC provides a Cybersecurity Assessment Tool (CAT) that offers a solid assessment framework that aligns with the level of maturity and complexity of Pacific College’s information system footprint. For even greater fidelity in the cybersecurity posture of their organization, Pacific College can use the [NIST SP 800-171A “Assessing Security Requirements for Controlled Unclassified Information”](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171a.pdf). Following the NIST SP 800-171A ensures that the assessment will be thorough and check the cybersecurity controls specified by the NIST SP 800-171 derived from the NIST SP 800-53.

Within the risk assessment, a detailed inventory of people, processes, data, hardware, and software should taken in order to **IDENTIFY** what needs protection. A business impact analysis (BIA) can then be performed in order to understand the true consequence (in monetary value) of viable exploitations. The BIA will provide insights into an appropriate IT and cybersecurity budget.

## Update Information System Security Plan (ISSP)

While Pacific College’s ISSP had quite a bit of material it was not without inaccuracies, inconsistencies, and omissions. To ensure that an updated ISSP provides a sufficient approach to ensuring the confidentiality, integrity, and availability of information and information technology it must be based on the asset inventory, risk assessment, and BIA mentioned above. Following an established template might be a good step in ensuring ISSP completeness and organization. NIST published an [ISSP template based on the NIST SP 171](https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-SSP-Template-final.docx). Ultimately, the ISSP should address all cybersecurity functions described in the NIST Cybersecurity framework: **IDENTIFY**, **PROTECT**, **DETECT**, **RESPOND**, and **RECOVER**.

The current ISSP describes the cybersecurity implementation (i.e. PROTECT), but it lacks detail regarding the monitoring of this baseline (i.e. DETECT), actions taken when a cybersecurity event occurs in order to contain the damage (i.e. RESPOND), and the procedures required to restore capabilities and services affected by an event (i.e. RECOVER).

In order to address the DETECT function of cybersecurity, a Continuous Monitoring Plan should be a section or an appendix to the ISSP. The NIST also publishes specific guidance on continuous monitoring in [NIST SP 800-137 “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.”](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf)

Establishing a capability to RESPOND to a cybersecurity event requires substantial planning and resources. The [NIST SP 800-61 rev 2 “Computer Security Incident Handling Guide”](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)  can assist in planning efficient and effective cybersecurity incident response. This publication provides guidelines for analyzing incident-related data and determining the appropriate response to each incident regardless of particular hardware platforms, operating systems, protocols, or applications.

Finally, recovering from a cybersecurity incident should be explicitly addressed in the ISSP. The [NIST SP 800-34 Rev. 1 “Contingency Planning Guide for Federal Information Systems”](https://csrc.nist.gov/CSRC/media/Publications/sp/800-34/rev-1/final/documents/sp800-34-rev1_cp_template_moderate_impact_system.docx) provides preventive measures, recovery strategies, and technical considerations required to restore information systems and their processing capabilities. This system-level planning should compliment facility-level disaster recovery planning (DRP) and organizational continuity of operations planning (COOP).

## Create Plan of Action and Milestones (POA&M)

Since resources are limited - money, time, manpower. A plan must be put together that communicates a “get well roadmap” to upper management. This plan must list open risks, appropriate countermeasures, their costs, and their priority. The implementation of a plan of action and milestone will have to take into account not only material costs and implementation time, but any training costs, impact of required system outages, or system testing.

See Appendix B for a POA&M example.

## Implement Server Security Standards

Pacific College, to their credit, utilize Amazon Web Services to host dozens of their operational servers (virtual machines [VMs]). However, the configuration of these servers is not in accordance with any industry standard. In order to harden these virtual machines, a safe, secure way to would be to deploy [ready-bake images from the Center for Internet Security](https://www.cisecurity.org/hardened-images/) then to layer the appropriate services onto these new VMs. Clearly, this process should not be conducted on the live servers, but in an integration and test environment, and a cutover would occur during off-peak hours.

The CIS images are configured to the [secure benchmarks](https://www.cisecurity.org/cis-benchmarks/), which  map to most major compliance frameworks such as the NIST Cybersecurity Framework and NIST 800-53. A mapping can seen at <https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf>.

## Implement Automated Vulnerability Scanning

It isn’t enough to establish a secure technical baseline. It must be monitored and maintained. To do this manually, even for a few servers, would be very arduous. As part of a would-be Continuous Monitoring Plan a vulnerability scanning and management tool like Tenable’s Nessus or Qualys’ Enterprise should be used to ensure that not only a secure configuration is maintained, but also when security patches are required.

The full Nessus enterprise solution may be excessive since its pricing begins for an enterprise solution with a $20K+ one-time license, plus $4K+ annual maintenance fee. This includes unlimited Nessus scanners, unlimited Passive Vulnerability Scanners and SecurityCenter. The more appropriate solution from Tenable would be the Nessus standalone with Professional feed that only costs $1,500. Qualys is a Software-as-a-Service (SaaS)offering that would cost roughly $300/year for an enterprise as small as Pacific College. (Tenable’s SaaS solution starts at over $2K)

Both solutions feature a broad range of 3rd party integrations. Qualys integrates with AWS and with Splunk - the industry leader for Security Information and Event Management (SIEM) tools while Nessus integrates with Salesforce - the Customer Relationship Management (CRM) tool. Both solutions leverage CIS benchmarks.

With cost being such a driving factor, the Qualys Enterprise seems like the most appropriate solution. This solution would be the cheapest AND fastest to implement.

# Conclusions

## Overall risk level

The risk level of this organization is HIGH.  The primary source of risk is the absence of necessary information security policies and programs and the lack of internal risk assessments and audits.  Only by completing and in-depth internal audit, as discussed under Recommendation #1, will the organization gain a full view of the current security posture and prioritize a way ahead.  Such an internal audit should make use of the standards referenced in this report (e.g., NIST SP 800-53/800-53A, the NIST Cybersecurity Framework, and/or the FFIEC Cybersecurity Assessment Tool (CAT)).  Conducting an annual audit will be beneficial in maintaining a clear picture of the organization’s risk and security posture and will help keep the organization’s security priorities aligned with the level and type of threats it faces.

## Plan / roadmap to get better

The recommendations contained in this reports will require a large investment of time, as well as some funding, to implement.  Making use of a framework (e.g.,the NIST Cybersecurity Framework or the FFIEC CAT), will help focus and prioritize efforts. The organization should develop a schedule, as described in the Recommendations section and Appendix B, to implement the recommendations as they deem necessary.

# Appendix A - Other Recommendations

**Implement a password policy**

An effective password policy should be included in the ISSP and should define required password length, complexity, age, and reuse of previous password.  Refer to guidance in NIST SP 800-63-3.

**Install anti-virus software on servers and workstations**

The organization has identified SentinelOne as its AV solution.

**Automated log review**

The site conducts periodic manual reviews of system and security logs, however, with greater than 20 servers the benefit of procuring log auditing software may be beneficial (e.g., Splunk: <https://www.splunk.com/en_us/software/splunk-cloud.html>) to meet NIST SP 800-53 AU-6 requirements.

**Configuration management**

The addition of a CM policy should be included in the updated ISSP.  Planned system changes should be reviewed by the ISSO to determine security implications prior to implementation.  See NIST SP 800-53 CM-1 and NIST SP 800-100 for program requirements. Servers baselines should be maintained in accordance with NIST SP 800-53 CM-2.

**Data-at-rest encryption**

The organization should determine data that requires additional protection through the use of a data classification system or other caveats (such as PII for personal student information or Confidential for the company’s intellectual property).  Segregation of different data types of classifications and the use of drive encryption software (e.g., BitLocker) can greatly reduce the negative consequence of a potential data breach. See NIST SP Rev. 4 SC-28 for requirements).

**Cybersecurity training program**

Implement a cybersecurity training program for staff members.  Employees should be trained upon hire and at recurring periods defined by the organization, which should not exceed one year.  Training for system administrators should be allocated in the IT budget to maintain the currency of security knowledge and skills.

**Data classification - PII, IP, etc.**

Data of varying type and sensitivity levels may require different storage and handling requirements.  The site should conduct a thorough review of the types of data it stores and determine if additional labeling and segregation of data is necessary.

**SW/HW inventory**

Maintain up to date HW/SW inventories per NIST SP 800-53 PM-5.

**Vulnerability alert service subscription**

A free subscription to one of many vulnerability tracking services, such as US CERT  (https://www.us-cert.gov), will provide regular security alerts, tips, and updates.

**Data breach insurance**

Include in the internal risk assessment a valuation of the potential loss the company would incur in the event of a data breach and determine the the need for insurance to transfer some of that risk if deemed necessary.

**Secure document transfer**

Make use of a secure portal for transferring documents containing PII.

**Disable SSL (web browsing and VPN use)**

The most current TLS protocols should be used for all transport security. See NIST SP 800-113 (Guide to SSL VPNs) and NIST 800-52 Rev. 1 (Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations).

# Appendix B - Sample POA&M

