Internal Audit engages in three primary activities – assurance audits, advisory services and investigations. The focus of our efforts is to assist management in the proper discharge of their duties by providing evaluation and feedback of internal control systems and operations.

This quarterly report includes update on the status of the current fiscal year audit plan and reports issued in the period. Current staffing includes CAE, Audit Manager, Sr. IT Auditor and three field auditors (one position is currently vacant since July – recruiting to begin in January).

<table>
<thead>
<tr>
<th>FY 2019 Audit Activity</th>
<th>Status</th>
<th>Completion of FY 2019 Audit Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>From FY 2019 Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Audit – PCard</td>
<td>E</td>
<td>C – Completed 0%</td>
</tr>
<tr>
<td>Continuous Audit – Travel</td>
<td>E</td>
<td>E – Engaged 60%</td>
</tr>
<tr>
<td>Continuous Audit – Gen Expense</td>
<td>E</td>
<td>N – Not yet Engaged 40%</td>
</tr>
<tr>
<td>Continuous Audit – Payroll</td>
<td>E</td>
<td></td>
</tr>
<tr>
<td>Time and Leave Reporting</td>
<td>N</td>
<td>Investigations – completed to report 0</td>
</tr>
<tr>
<td>Global Animal Health – Fiscal</td>
<td>E</td>
<td>Investigations – pending 3</td>
</tr>
<tr>
<td>Work Study</td>
<td>N</td>
<td>Investigations – closed in prelim 2</td>
</tr>
<tr>
<td>Disposal of Electronic Media</td>
<td>N</td>
<td>FY 2019 Investigations 5</td>
</tr>
<tr>
<td>CSC 9/11 – Secure Config. Of Network, Ports</td>
<td>N</td>
<td></td>
</tr>
<tr>
<td>CSC 15 – Wireless Access Points</td>
<td>E</td>
<td>Internal Advisories 36</td>
</tr>
</tbody>
</table>

At report date, several audits and investigations from prior year audit plans are in report stage or near completion. These will be included in future update reports as they are issued.

External Audit activities (not including various federal program audits occurring through year):

<table>
<thead>
<tr>
<th>Auditor</th>
<th>Scope</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>WA Ethics Board</td>
<td>Investigation – WSU Referral</td>
<td>Engaged</td>
</tr>
<tr>
<td>State Auditor (SAO)</td>
<td>FY 2016–2017 Accountability Audit – statutorily required</td>
<td>Close 11/18</td>
</tr>
<tr>
<td>State Auditor (SAO)</td>
<td>FY 2018 Financial Statement – contract</td>
<td>Engaged</td>
</tr>
<tr>
<td>CliftonLarsonAllen</td>
<td>FY 2017 Auxiliary Financial Statement – contract</td>
<td>Engaged</td>
</tr>
</tbody>
</table>

The following opinion methodology is applied to assurance audits:

<table>
<thead>
<tr>
<th>Satisfactory</th>
<th>Control Environment (CE) is adequate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some Improvement Needed</td>
<td>CE is adequate but some exceptions noted</td>
</tr>
<tr>
<td>Major Improvement Needed</td>
<td>CE not adequate and significant exceptions noted</td>
</tr>
</tbody>
</table>
Completed Reports Summary

P 17–11, IT Monitoring Logs and Accounts
Summary
The purpose of this Information Technology audit was to evaluate whether, specific to the cyber environment, event log collection, management, and analysis processes were adequate to help detect, understand, or recover from a cyberattack, and, that user, administrator and system accounts are properly managed throughout their life cycle. We found improvement is needed and rated two of seven issues as High risk. These were related to the policies and administration over accounts and passwords associated with Network ID and the financial system, including: password enforcement practices, gaps in policy or strength of policy, and enforcement of responsibilities when user roles change.

P 18–09, WSU Trademarks
Summary
The audit of WSU Trademarks was included in audit plan to evaluate whether management controls provide reasonable assurance that the University’s intellectual property in the form of logos, spirit marks and other unique branding are protected from abuse or misuse, and the University is receiving royalties due to it. For the period of review, $1.2 million in gross royalty revenues was generated. Overall the issues and the audited area were rated Low risk. Minor recommendations were communicated related to system access, review of third party contract terms and performance, and formalizing the role of the committee assigned responsibility for branding review and oversight.
Washington State University
Office of Internal Audit

Fiscal Year 2019 Audit Plan

Heather R. Lopez, CIA, CFE
Chief Audit Executive
Approved October 7, 2018
Table of Contents

Introduction ......................................................................................................................... 3
Planned Audits for Fiscal Year 2019 ................................................................................ 5
Other Types of Audits/Activities ....................................................................................... 7
Audit Resources .................................................................................................................. 9
Authority and Criteria ....................................................................................................... 11
Introduction

The Office of Internal Audit assists the University and management in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of its risk management, internal control and governance processes. These responsibilities include: performing reviews to provide reasonable assurance internal controls are adequate to safeguard resources, provide integrity and reliability in reporting, ensure adherence to compliance requirements and provide for efficiency and effectiveness in operations; assisting in the deterrence of fraud; advisory services that offer recommendations on systems of internal control and operations; and, advisory services to guide employees in the proper adherence to the Ethics in Public Service Act.

The Chief Audit Executive (CAE) reports functionally to the President and administratively to the Vice President for Finance and Administration. In accordance with the audit charter, the CAE is responsible for developing a flexible annual audit plan using appropriate risk-based methodology, including any risks or control concerns identified by management, and submitting that plan with periodic updates to the President for review and approval. In accordance with the charter and the Board of Regents Bylaws, the CAE also provides quarterly updates to the Finance and Compliance Committee regarding the audit plan and resource requirements, audit performance relative to the plan, and significant risk exposures and control issues, including fraud risks, governance issues and other matters of importance to senior management and the Board.

The purpose of the Audit Plan (the Plan) is to outline audits and other activities the WSU Office of Internal Audit will conduct during Fiscal Year 2019. The CAE is authorized to make changes to the Plan, as deemed necessary, to address changes in identified risks. The Finance and Compliance Committee and the President will be notified of any significant additions, deletions or other changes to the Plan.

The types of projects listed in the Plan demonstrate the variety of approaches Internal Audit takes to address its mission of assisting the University achieve its goals and objectives in an efficient and effective manner. Deliverables for audits and projects may include audit reports, technical assistance, data analysis, and other written and verbal communications.

Risk–based methodology

Audits and projects in the Plan were primarily identified through a University–wide risk assessment process designed to evaluate risks to the University’s strategic goals and initiatives. We interviewed key management to understand their views of the risk
environment and analyzed data across University accounts, areas and functions. We considered other risk inputs including recent audit results, external examinations, industry risk areas and alerts from sponsoring agencies and stakeholders. We also surveyed a population of 741 members of the University management community. This is a high-level risk survey that yielded a response rate of 47% (348 –same response rate as prior year) – 32% of these respondents provided additional write-in comments.

When we begin our audit planning and assessment activities we start with an audit universe. That universe includes auditable units, departments, centers, functions and operations. The universe is constantly evolving as University operations and strategic foci change. Each year, we update the universe periodically based on results of audit engagements (internal and external) and results of risk surveys and interviews weighted against defined risk factors. Applying weighted averages to the risk factors we ranked the top areas. Audit resources limit the number of audits that may be engaged during the year so risks are ranked in order of priority and against resource availability, with consideration of audits recently engaged or mitigating activities in place.

Occasionally, a risk area included in the Plan may have technical concerns beyond the expertise of the audit team. If additional resources (outsourced or co-sourced) are required to engage any audits, the CAE will work with the President to evaluate those needs. There are no audits included in this year’s Plan that will require outsourcing.

The specific scope of each audit in the Plan is determined once the audit team completes its audit planning process for each engagement. The engagement planning process includes consideration of the risk management, control, and governance processes in place to ensure:

- Accountability systems are in place to ensure organizational and program missions, goals, plans and objectives are achieved
- Risks are appropriately identified and managed
- Information is accurate, reliable and timely
- Employee actions are in compliance with policies, procedures and applicable laws and regulations
- Operations are effective and efficient
- Resources are acquired economically, used efficiently, and adequately protected
Planned Audits for Fiscal Year 2019

The following lists the projects included in this year’s Plan. They are not listed in rank order as some audits of higher ranking may not be available for engagement until later in the fiscal year due to client scheduling or other activities.

Our efforts are to ensure broad coverage of audit activity, including on-site audit engagement at all campuses. Although resources do not permit on-site review every year, the continuous audit program ensures continued test of decentralized transactions, and where feasible the key controls, in functional areas engaged at all campuses and sites.

Discussions with management and leadership have determined a greater investment of audit resources to assist in the positive preparation and transition to the University’s new finance and personnel system would provide great assistance. For this reason, we have carved out time from assurance engagements to perform the following activities that will not yield a final report with opinion on internal controls:

- **Advisory – Modernization:** We have allocated resources to assist management in two areas.
  1. Participate in planning meetings and workshops, providing feedback on controls, risks, process flows and design ideas for the implementation team.
  2. Review designed process flows and research/evaluate against impacted policies and procedures.

- **Self-Assessment Training and Development:** Again to assist with the modernization effort, but also to generally assist members of the fiscal and administrative community in maintaining a strong internal control environment. All internal audits start with a risk assessment and requests from management for their own assessments of risk against strategic plans and unit/function objectives. We have found more times than not, unit personnel are not familiar with COSO (internal control framework standard adopted by state of Washington and WSU). This project will continue our efforts to develop processes that units can utilize independent and per their own schedule to enhance internal control systems and processes and provide for continuous monitoring (and addressing) of risk at the various levels.

One more project that has been allocated resources that will not yield a control report or opinion is the development and implementation of an online ethics training program that will be deployed to meet the requirement for mandatory ethics training, university-wide.
This project will be engaged in close partnership with the WSU Assistant Attorney General's Office, Human Resource Services, and utilizing resources and feedback from the state Executive Ethics Board.

The following audit projects include test of controls and transactions at multiple locations unless a specific location is noted:

| Continuous Audit Program | The continuous audit program continues each year with the addition of different risk areas to test transactions for compliance, support and accountability. Data is pulled at intervals throughout the year from which test selections are made in the identified areas. For most audit subject areas, auditors perform a high-level review of all transactions for the scope area and period and select transactions based on high-risk criteria. At the end of the year, we have performed some form of analysis on all transactions in the defined area. This approach to audit makes better use of available audit resources while ensuring greater audit coverage of high-risk, usually decentralized functions or activities by active review for anomalies. Tests are applied to transactions regardless of physical location and usually cover all or most locations. The audit areas included in this year’s continuous program:
- Purchasing card
- Travel expenses
- General expenses
- Payroll |

| Time and Leave Reporting | As the university moves to implementing a new accounting system there will be a point where accrued leave balances, previously manually recorded, tracked and calculated, are entered into the new system as the new beginning balances. While the new system will have strong field controls to better provide assurance as to accuracy. We will expend efforts in decentralized areas to determine whether controls over monitoring and calculations of balances provide reasonable assurance that the ending balances are accurate before entry into the new system. |

| IT – Wireless Access Control (CSC 15) | This project was planned to be performed in year three of the five year IT Audit Plan but deferred to this fourth year due to resource limitations. This project is ranked 15 out of 20 in the SANS Center for Internet Security Top 20 Cyber Security Controls (CSC v6.1). |
### IT - Limitations and Control of Network Ports, Protocols and Services (CSC 9)

This project was planned to be performed in year three of the five year IT Audit Plan but deferred to this further year due to resource limitations. This project will combine two top ranked cyber risks (9 and 11) from the SANS Center for Internet Security Top 20 Cyber Security Controls (CSC v6.1). The test of the two areas is combined due to similar controls.

<table>
<thead>
<tr>
<th>Secure Configurations for Network Devices such as Firewalls, Routers and Switches (CSC 11)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Animal Health (GAH) has had increased activity in the past few years especially with the creation of non-governmental organizations (NGO) to facilitate international research and operations. External audits are required under the NGO agreements, grant terms or in-country requirements – and contracts with external firms are negotiated accordingly. Our review will focus on general operation and accounting functions and related controls as administered in the Pullman, WA offices and extended to in-country.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work-study jobs are to assist qualifying current students fund their education by finding part-time employment positions. Funding comes from federal and state sources. This project will review the University’s processes to ensure requirements of funding parties are met while achieving goals for assisting eligible students.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disposal of Electronic Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk survey results continue to rank data security concerns in the top 20. This project will review whether there are adequate controls to protect and remove confidential data residing on devices when custody is transferred – including copiers at end of lease, trade-ins, and assets sent to Surplus Stores.</td>
</tr>
</tbody>
</table>

### Other Types of Audits/Activities

### Follow-up Audits
Audits and formal investigations yielding a report with actionable recommendations will have a follow-up review conducted within the timeframe management indicates corrective actions will be implemented to evaluate response and adequacy of corrective action.

**Advisory Assistance/Consulting**

Internal audit staff may participate and/or assist University members in developing and maintaining strong governance, risk management, and control processes and systems. Activities may include serving as a member of a work group or committee, and providing consultative advice on financial, operational and compliance issues. Auditors also assist as audit liaison between the University and external audit groups.

**Ethics Advisor**

The Chief Audit Executive is the University’s Ethics Advisor. In this role, she serves as liaison between the University and the Washington State Executive Ethics Board, providing to University members guidance on ethics rules and advising on policy statements.

**Note:** WSU’s Office of Internal Audit follows the Standards promulgated by the Institute of Internal Auditors (IIA). New, effective January 2017, Standard 1112 CAE Roles Beyond Internal Auditing states, ‘Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence and objectivity.’ The CAE’s role as ethics advisor and the responsibilities related to promoting ethics are governance activities outside of internal auditing. Internal Audit is charged with evaluating the effectiveness of governance processes including the ethics and control environment. If the CAE holds responsibility for some of the governance processes to be evaluated then independence and objectivity may be impaired without appropriate safeguards.

**Issue:** Ethics and culture continue to rank high in risk surveys and during interviews with management. It is evident this area needs improvement.

**Recommendation:** It is recommended the University evaluate alternative processes to obtain assurance related to the effectiveness of the ethics program and its contributions toward a strong control environment.

**Enterprise Risk Management**

An ERM program strategically positions the University to better manage and direct resources to activities that are aligned with strategic goals and to mitigate risks to meeting institutional objectives. For an ERM program to work effectively and provide value, the process needs top down ownership, commitment and engagement. Internal Audit is well-positioned to help
facilitate the process given our experience in risk, assessment and broad engagement across all University units and operations. However, Internal Audit cannot own the process. The CAE will continue to partner with the Vice President of Finance and Administration to refine and enhance processes to achieve a robust, value-added and sustainable ERM program.

**Investigations**

Internal Audit reserves time in the audit budget for unplanned activities including investigations of misuse of funds or resources, malfeasance, misconduct, and ethics violations. Some investigations may be performed in collaboration with other investigatory units including Human Resource Services, Office for Equal Opportunity, Office of Research, Office of the Provost, Environmental Health and Safety, and the WSU Police Department. Occasionally, complaints of employee wrongdoing filed with the State Auditor’s Office via the Whistleblower program or the Citizen Hotline may be sent to Internal Audit for engagement or coordination.

**Audit Liaison**

Internal Audit serves as the coordination point for some external auditors including the State Auditor’s Office, the Executive Ethics Board and federal granting agencies. Liaison efforts include verifying purpose, authority and scope of audit, ensuring appropriate management is involved in audit activity, attending entrance and closing meetings, and evaluating results to determine if they are 1) accurate representations of activity and 2) indicators of systemic concerns that may need addressed with senior management.

**Audit Resources**

The Plan for Fiscal Year 2019 is based on a professional staffing complement of six auditors: three staff auditors, an IT auditor, an audit manager, and the Chief Audit Executive. There is, at the time of audit plan development, a vacancy with one of the staff auditor positions. This position is planned to be filled in January 2019 and accrued funds used towards recruitment of student interns in the spring. In the past, the Office has employed very talented and productive interns to assist with the continuous audit program. We hope to continue that success and the project budget does include use of interns in the spring semester.

Approximately 70% of Internal Audit’s available resources are committed to the completion of planned audit projects and follow-up audit procedures. The remaining 30% is held as contingency for unplanned activities such as consulting, liaison activities and investigations. Available resources include all workable hours per FTE less reserves for employee
professional development, administrative projects (e.g. internal quality improvement projects) and internal administration, including issues pertaining to personnel.

We have a few audit projects from prior year audit plans initiated but not yet completed. It is normal audit process to have a few audits begun in the last few months of the year completed and issued in the following year. Overall goal is to engage and complete 80% of planned audit areas and if time permits, all audits will be engaged.

Allocation of current year resources:

<table>
<thead>
<tr>
<th>Project</th>
<th>Estimated Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous – Purchasing Card</td>
<td>420</td>
</tr>
<tr>
<td>Continuous – Travel expenses</td>
<td>300</td>
</tr>
<tr>
<td>Continuous – General expenses (fund)</td>
<td>240</td>
</tr>
<tr>
<td>Continuous – Payroll</td>
<td>300</td>
</tr>
<tr>
<td>Time and Leave Reporting</td>
<td>700</td>
</tr>
<tr>
<td>Global Animal Health – Fiscal</td>
<td>500</td>
</tr>
<tr>
<td>Work Study</td>
<td>380</td>
</tr>
<tr>
<td>Disposal of Electronic Media</td>
<td>320</td>
</tr>
<tr>
<td>CSC 15</td>
<td>240</td>
</tr>
<tr>
<td>CSC 9/11</td>
<td>340</td>
</tr>
<tr>
<td>Self-Assessment Training and Development</td>
<td>240</td>
</tr>
<tr>
<td>Advisory – Modernization</td>
<td>220</td>
</tr>
<tr>
<td>Follow-up of Corrective Actions</td>
<td>200</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Hours</td>
<td>4,400</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project</th>
<th>Estimated Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation</td>
<td>500</td>
</tr>
<tr>
<td>Ethics Training Program Development</td>
<td>60</td>
</tr>
<tr>
<td>Advisory (Consulting, General Training)</td>
<td>280</td>
</tr>
<tr>
<td>External Audit Liaison</td>
<td>220</td>
</tr>
<tr>
<td>Committee Participation/Engagement</td>
<td>150</td>
</tr>
<tr>
<td>QAIP (Quality Assurance Improvement Program)</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Hours</td>
<td>1,290</td>
</tr>
</tbody>
</table>

Total Hours 5,690
Authority and Criteria

Auditing Standard
The WSU Office of Internal Audit follows standards promulgated by the Institute of Internal Auditors (IIA). In accordance with Standard 1000, the purpose, authority, and responsibility of the internal audit activity is formally defined in the audit charter. The charter includes the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing). The charter is periodically reviewed for revisions and any changes presented to the President for approval as required.

Standard 1300 requires the CAE to develop and maintain a quality assurance and improvement program (QAIP) that covers all aspects of the internal audit activity. The QAIP includes internal assessments such as regular supervisor monitoring of projects and activities and a newly implemented internal team member assessment of completed projects. External assessment includes a peer review to be conducted at least every five years.

Internal Control Framework
The University follows the COSO control framework and its guiding principles in the establishment of internal controls. The state of Washington has provided greater direction in the implementation of COSO for state agencies within the revised (effective July 1, 2017) Chapter 20 of the State Accounting and Administration Manual. Internal Audit strives to apply the COSO framework in tests of internal controls and provide appropriate direction and guidance to individuals.
June 21, 2018

Sasi Pillay  
Vice President of Information Technology Services and CIO  
Info Tech Bldg 2143  
P.O. Box 641222  
Pullman, Washington 99164–1222

Dear Vice President Pillay:

Following is the final report for our audit of IT Monitoring Logs and Accounts. Management’s response has been included in the report. We concur with the actions planned or already implemented.

In accordance with management’s estimated correction dates, we will perform follow-up activity to determine whether the corrective actions have been implemented and have achieved the desired effect.

We appreciate the cooperation and assistance provided by your staff during this review. Please let me know if we can be of further service.

Sincerely,

Heather Lopez  
Chief Audit Executive, Internal Audit

cc: Dr. Kirk Schulz, President  
Tony Opheim, Associate Vice President & Deputy CIO  
Tom Ambrosi, Chief Information Security Officer  
Stacy Pearson, Vice President Finance and Administration  
Danielle Hess, Division Chief, AAG
TABLE OF CONTENTS

EXECUTIVE SUMMARY ........................................................................................................... 3
BACKGROUND .......................................................................................................................... 4
SCOPE and AUDIT METHODOLOGY ..................................................................................... 5
ISSUES, RECOMMENDATIONS and MANAGEMENT RESPONSES ...................................... 6

1. Account Management (CSC 16) ......................................................................................... 6
   Issue 1.1: Password Enforcement Practice not Consistent with Executive Policy and not
   Working as Intended (NIST IA–5(1)), ................................................................................. 6
   Issue 1.2: Responsibilities are not Adequately Documented or Enforced (NIST AC–2), ...... 9
   Issue 1.3: Multifactor Authentication Standards are not Adequately Documented (NIST IA–
   5(11)) .................................................................................................................................. 11

2. Audit Logs (CSC 6) .............................................................................................................. 12
   Issue 2.1: Monitoring and Performance Objectives are not Formalized for Log Collection and
   Analysis Systems (NIST SI–4), ............................................................................................. 13
   Issue 2.2: Timestamp Granularity is not Defined in Policy or Procedure (NIST AU–8), ...... 14
   Additional Observation: ..................................................................................................... 14

3. University IT Governance .................................................................................................. 15
   Issue 3.1: Policy Review Practice not Consistent with Policy (NIST AC–1, IA–1, SI–1), ...... 15
   Issue 3.2: Logging Strategy not Documented in University–wide Policy or Procedure (NIST
   AU–1, OCIO 141.10.10.1), ................................................................................................. 16

CRITERIA, AUDIT STANDARDS, TEAM INFORMATION ....................................................... 18
APPENDIX A: Audit Risk and Opinion Methodology ............................................................... 20
APPENDIX B: Map of Critical Security Controls (CSC) to NIST Controls ............................ 21
APPENDIX C: Definition of NIST Controls Tested as Related to Policies and Procedures ....... 25
EXECUTIVE SUMMARY

The IT Monitoring Logs and Accounts audit was included in the Fiscal Year 2017 Audit Plan as a result of a risk assessment. The purpose of the audit was to ensure, specific to the cyber environment, event log collection, management, and analysis processes will help detect, understand, or recover from a cyber attack, and, that user, administrator and system accounts are properly managed throughout their life cycle.

Information Technology Services (ITS) is comprised of multiple departments responsible for various activities impacting the University as a whole. Included in these activities: administration of written IT policies; administration of event log collection, analysis and correlation activities; design, configuration and implementation of enforcement policies for user accounts.

Our audit objective was to evaluate whether internal controls as developed, approved and implemented provide reasonable assurance that:

- User, administrator and service accounts are actively managed throughout their lifecycle.
- Collection, management, and analysis of audit log events will help detect, understand, or recover from an attack.

Conclusion

Overall, we conclude internal controls are not adequate to ensure objectives are met.

In general, some improvement is needed in policy development and implementation. Detailed descriptions of issues in the following areas, including our recommendations and management’s responses, are provided within this report:

1. Account Management
2. Audit Logs
3. University IT Governance

We provided a risk rating for each of the issues identified – two of seven issues yielded a rating of High risk (see Appendix A).
BACKGROUND

Risk assessments were performed during FY 2015 to develop a Five Year IT Audit Plan (FY 2016–2020) that would strategically lay out an approach for reviewing the University system’s critical information technology controls. Although particular IT systems were not specified in the plan, further assessment is performed each year to best prioritize the IT systems and locations where tests will be performed in that year.

The critical information technology controls tested in this audit included:

- **Account Monitoring and Control**
  - Management process: Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

- **Audit Logs: Maintenance, Monitoring, and Analysis**
  - Management process: Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

The primary University information technology systems are supported by different system accounts including the Network ID (Windows Active Directory with federation), AIS User ID (mainframe access), and Unix Account (for web site administration). Almost all authentication and authorization is based on one of these three system accounts. Administrative accounts are also established for networking equipment separate from these forms however these types of accounts are only established for IT personnel with responsibilities for these systems.

As part of WSU’s Information Technology Services (ITS), the Information Security Services (ISS) group works 24x7x365 to protect the data resources of students, faculty and staff within the WSU community. Within the ISS group there is a key departmental goal of pursuing a standardized set of security solutions across the WSU campuses. Both the strategic and the departmental goals are supported by ITS/ISS efforts in the areas of event log monitoring using a SIEM (Security Information and Event Management) solution and account monitoring and control utilizing Active Directory for network user identification (NID).
SCOPE and AUDIT METHODOLOGY

The audit scope included ITS managed event log collection and analysis systems and Network ID (NID) user accounts. We did not perform tests specifically against AIS User IDs, however results of tests conducted within the audit scope did identify areas that need improvement related to AIS User ID management. Tests were performed on activities occurring during Fiscal Year 2018. Audit fieldwork took place between August 28, 2017 and March 14, 2018.

During the course of the audit we visited with Pullman ITS. We interviewed personnel responsible for five functions and identified and evaluated internal controls and operating procedures in effect at the time of audit fieldwork.

For password enforcement, we tested 7,978 user accounts against nine different password enforcement policies and compared those policies against the parameters defined in Executive Policy #18, Computer and Network User Identification and Password Policy.
ISSUES, RECOMMENDATIONS and MANAGEMENT RESPONSES

This section lists the issues presented to management. Each issue represents a condition, error or internal control weakness identified during the audit that may have a negative impact on the University’s or unit’s assets, financial information, and/or ability to comply with laws and regulations or University policies and procedures.

We summarized issues in the following general areas:

1. **Account Management**
2. **Audit Logs**
3. **University IT Governance**

For each issue, we prepared recommendations to address the situation and requested management’s plan for corrective action and a timeline for implementation.

We will follow up with management to determine whether corrective action has been implemented in the timeline established for each issue.

1. **Account Management** (CSC 16)

   Risk: Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network monitors.

   Methods to manage system accounts should include strong password management policies and procedures.

   *Control Objective:* Determine if the audit client has developed, approved and implemented controls that are adequate to ensure the active management of system accounts – their creation, use, dormancy, and deletion – in order to minimize opportunities for attackers to leverage them.

   **Issue 1.1:** Password Enforcement Practice not Consistent with Executive Policy and not Working as Intended (NIST IA-5(1)), *Audit Rating – High*
Specific to active directory accounts we found password enforcement policies configured in MGTHUB and ad.wsu.edu (both Fine Grained Password Policies (FGPP) and the Default Domain Policy (DDP)) are enforcing some parameters at levels that are more risky than those defined in Executive Policy (EP) #18.

In response to a 2015 data security incident, ITS, during their response and remediation efforts, implemented enhanced password enforcement conditions including a new methodology for domain administrator accounts (via mgthub domain) and multiple fine-grained password policies for different user and system accounts within ad.wsu.edu. During the process of configuring the settings for these enforcement mechanisms ITS evaluated usability needs, resulting in the modification of some enforcement parameters. When the enforcement parameters were modified the governing policies were not referenced or updated.

We found the following discrepancies between the various password enforcement policies in practice and those parameters as defined in EP#18:

- In current password enforcement policy, the Maximum Password Age for TEMP NID (FGPP) is set to 208 days, and, for AD Default (ad.wsu.edu) it is set to zero. An age limit of zero means no limit, so no requirement to change password. In EP #18, for general users, the Maximum Password Age is set to 180 days.
- In current password enforcement policy, the Maximum Password Age for Service Account Password is set to zero, so no limit. In EP #18, for these elevated users (administrators), the Maximum Password Age is set to 90 days.
- In current password enforcement policies, all but the AD Default Password Policy have higher lockout thresholds than in EP #18. Eight of nine enforcement policies are enforcing the lockouts at either 6, 150 or 500 attempts – meaning, for user with lockout set at 500, the user will be locked out and require administrative reset only after 500 failed logon attempts. In EP #18, the lockout threshold for all users is set to 5.
- For seven of the nine applied enforcement policies, the current setting for Minimum Password Age is set to zero. This creates a higher risk as it allows users to change their password enough times (24) in one day to return to their previous password. Minimum Password Lifetime is not defined in EP #18.
In addition, the following related issue was initially reported in the IT Data Access audit (report P 12–02, issued July 31, 2014) and remains unresolved:

- The AIS Mainframe is not configured to enforce password parameters.

This remains a significant risk as the AIS Mainframe is the university’s primary financial and personnel system.

To determine if the currently set enforcement policies are working as intended we tested 7,978 user accounts, comparing their password age against the maximum age parameter of the policy noted to be applied to the account. We found:

- In two cases, Tier1 Admin accounts were disabled but have their passwords manually set to never expire. If these accounts are re-enabled they will not be in compliance with password requirements.
- In two cases, currently active Domain Administrator accounts have been manually configured to have ‘never expire’ passwords.
- In 81 cases we found active NID (user) Accounts whose password ages exceeded the 180 maximum for general accounts defined in EP#18. They typically exceeded the age being enforced by the TEMP NID password policy (208 days) as well, leaving either the Service Account (elevated permissions) or AD Default (general permissions) Password policies as the ones being applied. Both of these policies have no age limit being enforced. This resulted in what appears to be the AD Default Domain Policy applying rather than the expected NID Password Policy being enforced. In discussing possible causes with ITS staff the belief is that the accounts were created during a window of time (late November 2015 through mid-July 2016) when an automated process stopped functioning properly. The process was fixed however, it appears the 81 accounts were not corrected.

**Conclusion**

Internal controls are not adequate to meet objective. Enforcing less secure parameters associated with passwords than those approved in EP #18 is a direct violation of that policy and increases the likelihood that credential theft efforts by cyber–attackers will succeed. Additionally it breeds confusion in the minds of users as to what University policy requirements are actually important and will be enforced. In turn this can result in an attitude of ambivalence towards other policies and fosters a lack of confidence in centralized IT administration by non–central IT departments and users in general.
### Recommendation

**ITS Management should review and correct discrepancies between practice and policy by modifying the enforcement policies, modifying Executive Policy #18, or a combination of the two.**

**Management Response and Corrective Action**

Estimated date for correction: ITS will create a draft BPPM by December 31, 2018.

### During review of EP #18, management should evaluate and apply an enforcement parameter or definition related to Minimum Password Age.

**Management Response and Corrective Action**

Estimated date for correction: Agreed – change to 1 day by August 3, 2018.

### Repeated Recommendation:

**The AIS Mainframe should be configured to enforce password parameters consistent with EP #18.**

**Management Response and Corrective Action**

Estimated date for correction: The AIS mainframe is an antiquated environment that cannot meet EP #18 requirements. This environment will be replaced by the end of FY2020. AIS will still exist in read-only mode through 2022. Current schedule for complete shutdown of AIS/mainframe is not until 2022.

### Issue 1.2: Responsibilities are not Adequately Documented or Enforced (NIST AC-2), Audit Rating – High

During the review of University-wide policies and during interviews with ITS staff we determined there are no specific policy requirements within WSU EPs or BPPMs that establish an account review frequency. Language in BPPM 85 sections 33 and 37 lack clarity and specificity about account management responsibilities including notification of when accounts are no longer needed, users transfer to a different department, and usage or need to know changes.

An automated process (ADW832) exists and appears to be working that detects when a current user’s status as an employee changes and, through a series of steps, updates this information in Active Directory to remove the former employee from their corresponding employee group. The AD updates do not modify the user’s membership in other AD groups.
where access permissions have been granted. These results are not sent to departmental personnel responsible for user account management nor to data owners or custodians for them to verify user access to the data they are ultimately responsible for managing.

This automated process does not extend to updating status for employees changing units or positions within the university. The current manual process for notifying ITS of an employee’s transfer from one department to another relies on the old department completing paper forms and routing them appropriately. If the form is completed and submitted to remove access there is the possibility that it could be processed after the access permissions for the new position have been provisioned. If this occurs access needed for the new position could be removed because access was initially granted for the old position and is now removed. An automated detective process can eliminate this type of event from occurring and notify all appropriate parties of the change.

Additionally, in two investigations (unrelated to this audit) and occurring in separate Colleges, common usernames and passwords were being shared by users. In both cases the IT departments supporting the systems at the time of the investigations did not know about the shared credentials. In both cases the computers being used with the shared credentials were not members of an administrative domain such as ad.wsu.edu or an equivalent departmental domain.

There are multiple causes for this situation including:

- Lack of detective controls implemented to identify when an employee has changed their job role.
- Lack of awareness (or willingness) on the part of Access & Authorization requestors to formally notify ITS of the change in an employee’s access needs.
- Lack of clearly defined and enforced University-wide account management responsibilities.

**Conclusion:**

Internal controls are not adequate to meet objective. Improper administration of user account access permissions increases the likelihood that user accounts will, over time, develop excessive access rights to data not needed for the user’s current job function. These excessive permissions increase the likely impact of a successful account compromise based cyber-attack (internally or externally initiated) due to the expanded
access to various data sets. The more data sets a compromised account has access to the greater the number of records that could be compromised resulting in potentially larger fines or penalties the University would be assessed.

<table>
<thead>
<tr>
<th><strong>Recommendation</strong></th>
<th><strong>Management Response and Corrective Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS management should enhance controls over user account administration by establishing, monitoring, and enforcing, periodic user account permission reviews within an EP or BPPM. The control enhancements should, at a minimum, define reviews to be performed, specific frequencies of reviews, who is responsible for conducting the reviews, and consequences for not performing the review.</td>
<td>Estimated date for correction: A replacement for EP18 by a BPPM is on the roadmap for FY19 which will address these controls.</td>
</tr>
<tr>
<td>Using logic similar to ADW832, ITS Management should develop, document and implement an account manager’s review report that will alert the appropriate account manager that position changes have occurred to accounts they are responsible for managing.</td>
<td>Estimated date for correction: We will investigate the current environment. However, there is a greater probability this can be accomplished in the new ERP in FY2021.</td>
</tr>
</tbody>
</table>

**Issue 1.3: Multifactor Authentication Standards are not Adequately Documented (NIST IA–5(11)), Audit Rating – Moderate**

ITS has deployed production token–based multifactor authentication processes in certain situations; however, there is no documented policy, procedure or guideline defining requirements or standards for Identity and Access Management token quality.

ITS management did not prioritize high enough the documentation of criteria, standards and objectives for their limited scope deployment of multifactor authentication.
Note: This is a repeat finding first reported in the IT Data Access audit (report P 12–02, issued July 31, 2014).

**Conclusion**

Internal controls are not adequate to meet objective. Implementation of new technologies, even those reported to resolve weaknesses in other implemented technologies, prior to documentation of standards, expectations and controls, increases the likelihood that the new technology will not perform as intended and may expose the University to unintended and unexpected risks.

<table>
<thead>
<tr>
<th><strong>Recommendation</strong></th>
<th><strong>Management Response and Corrective Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS Management should formally document and distribute accordingly, minimum requirements and capabilities of multifactor authentication mechanisms to be deployed. If, based on the data classification level of data being accessed, there are different requirements or capabilities these should be explicitly stated in the formal documentation.</td>
<td>Estimated date for correction: This will be researched and dealt with in the Okta MFA project in FY19.</td>
</tr>
</tbody>
</table>

2. **Audit Logs (CSC 6)**

Risk: Council on CyberSecurity, *Critical Security Controls for Effective Cyber Defense, v 5.0*, ‘Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines... Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. Sometimes logging records are the only evidence of a successful attack...Because of poor or nonexistent log analysis processes, attackers sometimes control victim machines for months or years without anyone in the target organization knowing, even though the evidence of the attack has been recorded in unexamined log files’.
Control Objective: Determine if the audit client has developed, approved and implemented controls that are adequate to ensure the collection, management, and analysis of audit log events will help to detect, understand, or recover from an attack.

Issue 2.1: Monitoring and Performance Objectives are not Formalized for Log Collection and Analysis Systems (NIST SI-4), Audit Rating – Moderate

State of Washington OCIO Policy 141.10 states agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system.

During review of existing university-wide IT policies we found no formal monitoring objectives have been developed, documented or distributed to appropriate individuals. At a minimum, objectives should address detection and identification of: attacks; indicators of potential attacks, unauthorized local, network and remote connections; and unauthorized use of a system. Additionally, techniques and methods to identify unauthorized use should be defined.

ITS has developed a departmental standard “ITS Information System Audit Logging Standard” however, it does not address the objectives of implementing and operating a log collection and analysis solution. During response and remediation efforts associated with a 2015 event, ITS rapidly deployed logging components across the University. This was a tactical implementation given the situation at the time. This was not followed up with a strategic governance mindset to document and implement long term objectives and methodologies.

Conclusion
Internal controls are not adequate to meet objectives. Lack of appropriate monitoring and performance objectives reduces management's ability to measure the effectiveness of existing audit logging activities and to make improvements to those activities to ensure the University is receiving appropriate benefits for the investment.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Management Response and Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS management should develop, document and distribute to appropriate individuals objectives for the various monitoring activities and establish appropriate program</td>
<td>Estimated date for correction: This will be researched and addressed in FY19.</td>
</tr>
</tbody>
</table>
**performance objectives to assist in evaluating the effectiveness of audit logging activities.**

---

**Issue 2.2: Timestamp Granularity is not Defined in Policy or Procedure (NIST AU-8), Audit Rating – Low**

During review of existing IT policies we found granularity of timestamps for event logs has not been defined University-wide in either an Executive Policy or in the BPPMs. The ITS departmental standard for event logging "ITS Information System Audit Logging Standard" also does not address the topic of timestamp granularity.

ITS management has not prioritized high enough the documentation of timestamp criteria for the University at least in part due to advances in time protocol implementation across modern operating systems being able to track time events to the millisecond.

**Conclusion**

Internal controls are not adequate to meet objective. Imprecise timestamps on logged and analyzed events have a negative effect on the performance and accuracy of SIEM systems used to analyze, correlate and alert on reported events.

<table>
<thead>
<tr>
<th><strong>Recommendation</strong></th>
<th><strong>Management Response and Corrective Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ITS management should incorporate language regarding timestamp granularity into an existing or new EP or BPPM (see issue 2 Logging Strategy) or for the interim, modify the departmental standard to incorporate such language.</td>
<td>Estimated date for correction: ITS does not believe this should be addressed in an Executive Policy or BPPM. ITS will address this issue in a proposed WSU standard by October 1, 2018.</td>
</tr>
</tbody>
</table>

**Additional Observation:**

In December 2017 efforts to migrate the mainframe processing to a cloud-hosting provider were completed. During the project, ITS Leadership evaluated installation of an event forwarder to send the event logs from the mainframe into the Splunk SIEM system for analysis.
ITS Leadership determined that the cost of the agent exceeded the value of the benefits WSU would receive. There was no agent installed while the mainframe was located in Pullman so from this perspective there was no improvement or degradation of existing controls and administrators still have the same mainframe event log access that they had prior to the migration effort.

3. University IT Governance

**Control Objective:** Audit objective was to determine if the audit client has developed, approved and implemented controls that are adequate to ensure that frameworks or methodologies are in place to support a safe and secure computing environment.

**Issue 3.1: Policy Review Practice not Consistent with Policy (NIST AC-1, IA-1, SI-1), Audit Rating – Moderate**

Executive Policy #5 (EP #5) defines the policy review period for the University at a minimum of every three years.

During test of when IT policies were last reviewed we found 4 out of 5 policies have not been reviewed within the defined time period. One policy is currently under review and is just over the 3 year cycle.

EP #5 Policy Approval and Distribution was updated in September 2014 to include the 3 year cycle as a minimum frequency. ITS management has not yet fully incorporated the new minimum 3 year policy review process into their standard operating procedures.

The specific policies and procedures reviewed and found to not meet the requirements are:

- EP #8 University Data Policies (February 5, 2015 – currently under revision)
- EP #14 University Antivirus Policy (February 4, 2002)
- EP #18 Computer and Network User Identification and Password Policy (December 2, 2005)
- ITS Information System Audit Logging Standard (February 5, 2015)

**Conclusion**

Not reviewing policies in a timely manner can result in policies not reflecting the current IT operating environment.
### Recommendation

**ITS management should implement appropriate processes to ensure all IT related policies and procedures (departmental as well as University-wide) are reviewed within the three year cycle defined in EP#5 or the frequency defined in the policy/procedure/standard document and that the review is appropriately documented.**

### Management Response and Corrective Action

**Estimated date for correction:**

ITS will create a roadmap for updating and developing new EP/BPPM and are planning on following that schedule by December 31, 2018.

---

### Issue 3.2: Logging Strategy not Documented in University-wide Policy or Procedure (NIST AU-1, OCIO 141.10.10.1), Audit Rating – Moderate

State of Washington OCIO Policy 141.10 states agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system.

During review of existing Executive and BPPM IT policies we found no discussion relating to event log strategies.

ITS management has not prioritized at a high enough level the development and documentation of a University-wide logging strategy.

This is an aggregated issue, components of which were first reported in the IT Data Access audit (report P 12-02, issued July 31, 2014) and remain unresolved or inadequately addressed:

- Lack of an adequate policy or procedure establishing the frequency of information system audit record reviews and analyses.
- Lack of an adequate policy statement defining the frequency for information system account review.
- Lack of an adequate policy, policy statement or procedure that addresses system audit and accountability standards.
- Lack of an adequate policy or procedure that identifies minimum levels of system logging and audit capabilities.
None of the IT–related Executive Policies (EP) nor the Business Policies and Procedures Manual (BPPM) establish and document a logging strategy for University IT systems. This is a violation of State OCIO Policy 141.10.

Conclusion

Internal controls are not adequate to meet objective. Inconsistent logging of events diminishes the effectiveness of Security Information and Event Management solutions and can cause delays in detecting inappropriate or adversarial activities occurring within the WSU environment.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Management Response and Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>While there is a departmental standard (ITS Information System Audit Logging Standard) developed, ITS management should formalize in EP or BPPM a policy and supporting procedures that establishes standardized minimum audit logging parameters for University IT systems. The strategy should be based on the risks and complexity associated with the data or system being monitored.</td>
<td>Estimated date for correction: ITS will address this issue in a proposed WSU standard by October 1, 2018.</td>
</tr>
</tbody>
</table>
CRITERIA

During the course of our review we referred to the following rules, regulations and/or policies:

WSU:
- EP #8 University Data Policies
- EP #13 Wireless LAN Policy
- EP #14 University Antivirus Policy
- EP #16 University Network Policies
- EP #18 Computer and Network User Identification and Password Policy
- BPPM 85 Computing and Telecommunications

Office of the Chief Information Officer, Washington State
- 141 Securing Information Technology Assets
- 141.10 Securing Information Technology Assets Standards

Federal or Industry Standards:
- SANS Top 20 Critical Security Controls v5 – Is an alternate industry standard methodology for grouping critical security controls into related categories that provides for a more holistic relationship for assessing and implementing controls and is viewed by the CISO as an approach that will likely foster quicker and broader adoption of IT security controls by the University.
- NIST SP 800–53r4 – Is an industry standard security controls catalog that maps IT security controls to the security impact associated with information and information systems. It offers a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate – contributing to systems that are more resilient in the face of cyber-attacks and other threats.

AUDIT STANDARDS

Our office follows the guidelines as promulgated by the Institute of Internal Auditors’ “International Standards for the Professional Practice of internal Auditing” (IIA Standards), in carrying out the planning and engagement of audit activity. The IIA Standards required we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis
for our findings and conclusions based on our audit objectives. Accordingly, we included such tests of the records and other procedures as we considered necessary in the circumstances.

The WSU Office of Internal Audit is not in full conformance with the IIA Standards in that a quality peer review has not yet been performed.

AUDIT TEAM INFORMATION

Internal auditors assigned to the audit include:

   Lead Auditor        Kevin Ulstad

The audit was supervised by Heather Lopez.

For questions regarding this project, contact  Heather Lopez, Chief Audit Executive:

   Email:  hlopez@wsu.edu
   Phone:  (509) 335–2001
   Website:  http://www.internalaudit.wsu.edu
### APPENDIX A: Audit Risk and Opinion Methodology

<table>
<thead>
<tr>
<th>Rating</th>
<th>Audit Risk Rating Criteria</th>
</tr>
</thead>
</table>
| **High** | Risk has a high impact and is highly likely to occur  
This is a high-priority issue – immediate management attention is required. This is a serious internal control or risk management issue that if not mitigated, may, with a high degree of certainty, lead to:  
- Substantial losses, possibly in conjunction with other weaknesses in the control framework or the organizational entity or process being audited  
- Serious violation of University strategies, policies, or values  
- Serious reputation damage, such as negative media publicity  
- Significant adverse regulatory impact, such as loss of operating licenses or material fines |
| **Moderate** | Risk has a high impact and low likelihood, or low impact and high likelihood  
This is a medium-priority issue – timely management attention is warranted. This is an internal control or risk management issue that could lead to:  
- Financial losses  
- Loss of controls within the organizational entity or process being audited  
- Reputation damage, such as negative publicity in local or regional media  
- Adverse regulatory impact, such as public sanctions or immaterial fines |
| **Low** | Risk has a low impact and low likelihood  
This is a low-priority issue – routine management attention is warranted. This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the unit or process being audited. Risks are limited. |

### Areas of Proficiency  
Positive statements where internal controls, governance or risk management processes were adequately established and functioning well for each of the audited area/systems.

### Table of Opinion Methodology

<table>
<thead>
<tr>
<th>Opinion Methodology</th>
<th>Criteria</th>
</tr>
</thead>
</table>
| **Satisfactory**   | - Control environment is adequate  
- No findings noted  
- Management’s control environment appears sound  
- All high-level risks adequately controlled |
| **Some Improvement Needed** | - Control environment is adequate but some exceptions exist  
- Some control weaknesses and/or opportunities for improvement observed  
- Management’s control environment appears otherwise sound  
- High-level risks are adequately controlled |
| **Major Improvement Needed** | - Control environment is not adequate and significant exceptions exist  
- Some high-level risks are not adequately controlled  
- At least one finding is rated “high”  
- Immediate safety and soundness are not threatened, but management’s control environment requires improvement  
- Significant exposure to fraud or security vulnerabilities |
APPENDIX B: Map of Critical Security Controls (CSC) to NIST Controls, Description of Controls Tested and Results

SANS Top 20 Critical Security Controls v6.1 is an alternate industry standard methodology (created in collaboration with CIS – Center for Internet Security) for grouping critical security controls into related categories that provides for a more holistic relationship for assessing and implementing controls and is viewed by WSU’s CISO as an approach that will likely foster quicker and broader adoption of IT security controls by the University.

NIST SP 800–53r4 is an industry standard security controls catalog that maps IT security controls to the security impact associated with information and information systems. It offers a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate. This approach contributes to systems that are more resilient in the face of cyber-attacks and other threats.

CSCs selected for testing: CSC 6 (CSC 14 in SANS Top 20 v5) and 16 with individual controls within each control group selected as relevant to organization activity and priority or impact levels.

**CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs**

*Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.*

<table>
<thead>
<tr>
<th>SANS 6.1 ID</th>
<th>Description</th>
<th>NIST Control</th>
<th>Description</th>
<th>Results of Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.</td>
<td>AU–8</td>
<td>Time Stamps</td>
<td>X</td>
</tr>
</tbody>
</table>


| 6.2 | Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format. | AU-2 | Audit Events | X |
| 6.3 | Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis. | AU-3 | Contents of Audit Records | X |
| 6.4 | Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings. | AU-5 | Response To Audit Processing Failures | X |
| 6.5 | Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device. | AU-6 | Audit Review, Analysis, And Reporting | X |
6.6 Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

CSC 16: Account Monitoring and Control

*Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.*

<table>
<thead>
<tr>
<th>SANS 6.1 ID</th>
<th>Description</th>
<th>NIST Control</th>
<th>Title</th>
<th>Results of Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.1</td>
<td>Review all system accounts and disable any account that cannot be associated with a business process and owner.</td>
<td>AC-2</td>
<td>Account Management</td>
<td>X</td>
</tr>
<tr>
<td>16.2</td>
<td>Ensure that all accounts have an expiration date that is monitored and enforced.</td>
<td>AC-3</td>
<td>Access Enforcement</td>
<td>X</td>
</tr>
<tr>
<td>16.6</td>
<td>Monitor account usage to determine dormant accounts, notifying the user or user’s manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff.</td>
<td>IA-5</td>
<td>Authenticator Management</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IA-5(1)</td>
<td>Password-Based Authentication</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IA-5(11)</td>
<td>Token-Based Authentication</td>
<td>X</td>
</tr>
</tbody>
</table>
Security or system administrators should then disable accounts that are not assigned to valid workforce members.

| 16.8 | Monitor attempts to access deactivated accounts through audit logging. | SI–4 | Information System Monitoring | X |
APPENDIX C: Definition of NIST Controls Tested as Related to Policies and Procedures

NIST SP 800–53r4 is an industry standard security controls catalog that maps IT security controls to the security impact associated with information and information systems. It offers a holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate. This approach contributes to systems that are more resilient in the face of cyber-attacks and other threats.

The following controls are not specific to the Critical Security Controls tested within this audit but instead are more broadly applied at the organization level. The noted controls address the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards and guidance. Security program policies and procedures at the organization level may make the need for system–specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or, conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

<table>
<thead>
<tr>
<th>NIST Control</th>
<th>Description</th>
<th>Results of Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC–1</td>
<td>Access Control Policy and Procedures</td>
<td>X</td>
</tr>
<tr>
<td>AU–1</td>
<td>Audit and Accountability Policy and Procedures</td>
<td>X</td>
</tr>
<tr>
<td>IA–1</td>
<td>Identification and Authentication Policy and Procedures</td>
<td>X</td>
</tr>
<tr>
<td>SI–1</td>
<td>System and Information Integrity Policy and Procedures</td>
<td>X</td>
</tr>
</tbody>
</table>
September 5, 2018

Stacy Pearson
Vice President for Finance & Administration
French Ad 442
Pullman, Washington 99164–1045

Dear Vice President Pearson:

Following is the final report for our audit of WSU Trademarks. Management’s response has been included in the report. We concur with the actions planned or already implemented.

We will perform a follow-up review, according to timelines of implementation identified by management, to determine whether the corrective actions have achieved the desired effect.

We appreciate the cooperation and assistance provided by your staff during this review. Please let me know if we can be of further service.

Sincerely,

Heather Lopez
Chief Audit Executive, Internal Audit

cc: Dr. Kirk Schulz, President
Victoria Murray, Executive Director, Finance and Administration
Alyce Anderson, Program Admin Manager, Trademarks
Matt Skinner, Associate Vice President/Internal Control Officer, AVPFS
Danielle Hess, Division Chief, AAG
# Table of Contents

EXECUTIVE SUMMARY .......................................................................................................................... 3
BACKGROUND ........................................................................................................................................ 4
SCOPE and AUDIT METHODOLOGY ..................................................................................................... 5
ISSUES, RECOMMENDATIONS and MANAGEMENT RESPONSES .................................................. 6
CRITERIA .................................................................................................................................................. 11
AUDIT STANDARDS ................................................................................................................................. 12
AUDIT TEAM INFORMATION ................................................................................................................. 12
EXECUTIVE SUMMARY

The audit of Washington State University (WSU) Trademarks was included in the Fiscal Year 2018 Audit Plan as a result of risk assessment. The purpose of the audit was to review effectiveness of the processes in place to control the University’s intellectual property – Trademarks.

The Trademark Licensing office, a unit of Finance & Administration, is primarily responsible for the Trademark Licensing program. The Trademark Licensing office coordinates and reviews requests to apply the University’s identity to products. Revenues generated through sales of licensed merchandise support WSU’s programs and services. For the audit period of FY 2017, there were 367 approved licensed vendors, from whom $1.2 million in gross royalty revenues was generated.

Our audit objective was to evaluate whether internal controls as developed, approved and implemented provide reasonable assurance that:

- The University’s intellectual property in the form of logos, spirit marks and other unique branding are protected from abuse or misuse
- The University is receiving royalties due to it and adequately controlling that revenue stream

Conclusion

Overall, we concluded internal controls were adequate to meet noted objectives.

While some improvement is needed, all issues included within this report have been rated as low risk. Detailed descriptions of the following issues, our recommendations, and management’s responses are provided within this report:

Issue 1: Access to Licensee Site Is Restricted to One User
Issue 2: Review of Third-Party Contract Terms Is Not Performed Timely or Complete
Issue 3: Review of Third-Party Performance to Contract Terms Is Incomplete
Issue 4: Branding Committee Role Is Not Formally Defined
BACKGROUND

At WSU, the Trademark Licensing office, a unit of Finance and Administration (F&A), has developed policy (Intellectual Property policy, BPPM 35.10, on use of WSU Name and Trademarks) to govern the use of WSU’s name and trademarks. All licensing decisions to approve or deny use of WSU trademarks are made by Trademark Licensing, an office with one full-time staff member and one part-time appointment. Fiscal management and oversight, including revenue receipt and posting, is provided by the F&A Business Office.

WSU has contracted with The Collegiate Licensing Company (CLC), now IMGCL (IMG College Licensing – due to IMG acquiring CLC), to act as WSU’s agent. IMGCL promotes the production of quality, licensed products, and facilitates licensee royalty revenue collection and overall reporting. IMGCL also audits licensees to ensure accuracy in royalty reporting and helps to monitor abuse and misuse of WSU’s trademarks. In addition, IMGCL has partnered with JPatton, which provides total brand protection through customized product authentication to enforce WSU’s brand protection program.

The Trademark Licensing office is assisted by a contracted Special Assistant Attorney General (SAAG) who helps with the monitoring and filing of new registration and renewals of WSU’s trademarks through the United States Patent & Trademarks Office (USPTO) for U.S. registrations and with corresponding agencies for registrations in Canada and Japan.

The Trademark Licensing office is also supported by the informal Branding Committee, legal counsel at WSU and WSU Police in enforcing compliance and protecting the University’s trademarks. Overall, there are 367 approved licensed vendors who have completed the application process, obtained approval and entered into an agreement with IMGCL to use the University’s trademarks in accordance with the contract terms. Royalty revenues generated through these vendors (licensees) have experienced a gradual increase over the last four years (from $920,738 in FY 2014 to $1.2 million in FY 2017). These amounts are prior to any deductions or transfers. The net licensing revenues are split evenly between Athletics and F&A.
SCOPE and AUDIT METHODOLOGY

The audit scope included review of the University’s trademarks including its name, spirit marks and logos. Tests were performed on transactions occurring during FY 2017. Audit fieldwork took place between May 17, 2018 and June 29, 2018.

During the course of the audit, we visited the Trademark Licensing office and the F&A office. We interviewed unit personnel and identified and evaluated internal controls and operating procedures in effect at the time of audit fieldwork.

We tested and reconciled FY 2017 royalty revenue transactions to contract terms and as reported in the FY 2017 Annual Report provided by IMGCL.

We tested twenty-one licensees in the following areas:

- Review of approved/denied licensee applications for completeness in review and approval process, supported and approved/denied timely
- Monitoring of approved licensees for renewals, reasons for termination/cancellation and close-out procedures followed

In addition, we reviewed the role and responsibility of the Branding Committee in brand protection and review of third-party contracted agents’ (IMGCL and SAAG) contract terms in safeguarding WSU trademarks.
ISSUES, RECOMMENDATIONS and MANAGEMENT RESPONSES

The following lists the issues presented to management. Each issue represents a condition, error or internal control weakness identified during the audit that may have a negative impact on the University’s or unit’s assets, financial information, and/or ability to comply with laws and regulations or University policies and procedures.

For each issue, we prepared recommendations to address the situation and requested management’s plan for corrective action and a timeline for implementation.

We will follow up with management to determine whether corrective action has been implemented in the timeline established for each issue.

**Issue 1: Access to Licensee Site Restricted to One User – Low Risk**

Personnel at the Trademark Licensing office use the system, Brand Manager 360 (BM360), provided by IMGCL to review license applications, approve/deny licensees, monitor license renewals and terminate/cancel licensees. The same system is also used to generate reports for monitoring royalty revenues.

WSU has been provided only one user account to access the BM360 system. Management noted that although there was only one primary user, two other individuals performing some form of processing and administration over trademarks could easily request the primary user access the system for reports or agreements. Not having a second user account limits the ability for secondary oversight and management.

Because there is only one user account, there are times when the primary user is unavailable and the user access and password has been shared with other users. University policy (at Executive Policy #18, and as aligned with best practices in data security) provides that passwords “shall not be shared or transferred to others” and it is the responsibility of users to keep passwords secret.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Management Response and Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>The unit should determine feasibility of adding a second user account to access the BM360 system, to provide for at least one backup user and facilitate access for secondary review and oversight.</em></td>
<td><em>Absent the ability to have multiple user accounts within the BM360 system, we will establish a system to indicate and track who has reviewed submissions. There are only two users of the BM360 system, and any</em></td>
</tr>
<tr>
<td><strong>Issue 2:</strong> Review of Third-Party Contract Terms Is Not Performed Timely or Complete – Low Risk</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
</tr>
</tbody>
</table>

In 2003, WSU entered into an agency agreement with CLC (now IMGCL) and with CLC International to act as WSU’s agent to license the use of WSU indicia to licensed vendors, to market and conduct certain promotions in such a manner as to preserve the integrity, character and dignity of the University and maintain the reputation of the indicia through high quality merchandise. The contractor is also responsible for collecting royalty revenues from
licensed vendors and remitting contractually agreed amounts to WSU. Addendums to the agreement were signed in 2008, 2010 and 2013.

While the contract has not been formally amended since 2013 we did note interim efforts by management to evaluate the contract and look for the best terms for WSU as applicable to royalty revenue allocation amounts. However, during our review of the details of the IMGCL contract and its addendums, we noted a few inconsistencies indicating a need for more timely and diligent review: name of contact for receipt of royalty revenue checks was incorrect (named an employee who separated from WSU over 11 years ago), and, terms of CLC International agency agreement had expired (06/30/2013).

There has been turnover in the F&A office and responsibilities for oversight of the trademark program reassigned. Not having an established transition process in this instance resulted in lack of monitoring of contract terms to ensure they are current and renewals are processed timely.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Management Response and Corrective Action</th>
</tr>
</thead>
</table>
| **Trademark Licensing Office and F&A should improve processes for timely and thorough review of contracts to ensure terms and requirements fulfill University expectations. This includes implementing a process to ensure contract review when there is transition of oversight to other units or personnel.** | Contract review will be conducted and documented in January of each year. If or when there is a transition in oversight, at either executive or management level, the contract will be reviewed and updated with appropriate contact information.  
   *Estimated date for correction: Jan. 31, 2019*                                                                 |
| **Current contract and addendums need corrected and updated.**                                                                                 | A comprehensive review of the current contract and addenda will be completed, and updated as necessary.  
   *Estimated date for correction: Jan. 31, 2019*                                                                                           |

**Issue 3: Review of Third-Party Performance to Contract Terms Is Incomplete – Low Risk**

Approvals for use of indicia, type of products and the distribution channels to be used are routinely processed and approved by the Trademark Licensing office in coordination with IMGCL. The third-party contractor initiates renewal processing, collects royalty revenues from
licensees and remits to WSU after a fee deduction. In addition, the contractor ensures performance of close-out processes occur within 60 days of licensee termination/cancellation and performs audits as applicable.

We reviewed a judgmental selection of licensees that were near their contract expiration dates. For the one international licensee, we noted a discrepancy in registration term and length of period. The request to renew was approved and processed by both the Trademark Licensing office and IMGCL despite the discrepancy. In the event of contract dispute it would be difficult to ascertain which terms should be applied.

We reviewed a judgmental selection of terminated/cancelled licensees to examine monitoring of the close-out process. The third-party contractor provides information on licensees that have terminated/cancelled, but there is little to no information provided to WSU that close-out processes were performed and Trademark Licensing personnel did not have a process in place to request that information. Thus, the Trademark Licensing Office was unable to provide results of the close-out process required to be conducted by IMGCL.

We reviewed and reconciled royalty revenues to contract terms for timeliness in royalty remittance, accuracy in percentage of administrative and collegiate marketing fund deductions and royalty revenue reporting. Although we found no variances, there was no evidence of a reconciliation process to verify the received amounts and as noted on remittance aligned with contracted percentages and deductions.

<table>
<thead>
<tr>
<th><strong>Recommendation</strong></th>
<th><strong>Management Response and Corrective Action</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes for monitoring of licensee activity from initial approval, renewal and final close-out at termination/cancellation should be improved to ensure adequacy in managing and providing safeguard to the institution’s trademark program.</td>
<td>The process for initial approval of licensees is very well documented and readily tracked within the BM360 system. While WSU staff are actively involved in renewal and close-out decisions, the processes for renewal and final close-out are not as readily viewable within the system. Thus, we will request copies of all renewal and closeout documentation moving forward.</td>
</tr>
</tbody>
</table>

*Estimated date for correction: Complete*
Results of monitoring close-out reviews and audits should be maintained to support review of performance of contracted services.

Audits are conducted on a three year rotation and results are outlined in the royalty reports. Close-out reviews are conducted by IMGCL upon license termination. As part of the close-out process, IMGCL maintains a checklist. Moving forward, we will request a copy of that checklist and any related communications to assist us in the review of their services.

*Estimated date for correction:* Complete

<table>
<thead>
<tr>
<th>Establish documented processes for royalty revenue reconciliation and other calculations to ensure proactive monitoring and verification of accuracy and completeness against contracted terms.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once quarterly reports and royalty revenue payments are received, staff will cross-check with the Insights system for consistency, and will also calculate the IMGCL fee for accuracy and consistency with contractual terms. Staff completing this step will initial and date the report. Secondary review of the payment occurs in Finance and Administration as part of the deposit process, and staff completing this review will initial the report and attach to the deposit report.</td>
</tr>
<tr>
<td><em>Estimated date for correction:</em> Oct. 31, 2018</td>
</tr>
</tbody>
</table>

**Issue 4: Branding Committee Role Is Not Formally Defined – Low Risk**

The Trademark Licensing program is responsible for protecting the use of WSU trademarks and for licensing commercial use of the marks. The program ensures that each use of the University's name is professional, tasteful and of a quality that reflects positively on the University.

The Trademark Licensing office collaborates with the Product & Art Approval Committee, also known as the Branding Committee, to ensure artwork used by approved licensees and by other internal users aligns with the University’s vision and mission of reputation, image and brand identity.
The five-member committee is ad hoc and collaborates on an, at times, daily basis over appropriate use of WSU’s trademarks. The University Marketing and Communications office has developed Academic Brand Guidelines, while the Athletic Brand Guidelines were developed by Nike in collaboration with the Trademark Licensing Office. The Branding Committee refers to these guidelines while reviewing artwork requests to ensure use of WSU brand aligns and identifies with WSUs reputation and mission. They meet periodically in person to discuss big agenda items. The members are part of the brand listserv and respond to questions from the public on appropriate use of the University brand.

The committee is entrusted with a critical role in monitoring the guidelines and ensuring alignment for non-Pullman campus use of WSU trademarks. However, the committee does not have bylaws delineating member composition, terms and functions. During audit fieldwork it was noted one member had separated – yet the committee had no process for identifying and selecting a replacement. There were no guidelines for committee member roles and no authorization for their existence and/or authorities.

As a result, committee meetings were ad hoc and informal, making it difficult to assign responsibility over functions. Absence of committee bylaws or guidelines makes it difficult to determine member participation and their effectiveness in discharging their committee roles.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Management Response and Corrective Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Should Trademark Licensing determine the services of the Branding Committee are critical to the program, there should be formal designation recognizing their role and expected member composition, term and functions.</td>
<td>Trademark Licensing staff will take the lead role in formalizing the Branding Committee to include representatives from University Communications, Publications and Printing, Athletics, and Trademark Licensing.</td>
</tr>
<tr>
<td></td>
<td>Estimated date for correction: Mar. 1, 2019</td>
</tr>
</tbody>
</table>
CRITERIA

During the course of our review we referred to the following rules, regulations and/or policies as a basis for our testing but are not all inclusive:

WSU Brand Standards
WSU Trademark Licensing
BPPM 35.10 Use of Washington State University Name and Trademarks
Collegiate Licensing Company (CLC)
US Patent & Trademark Office (USPTO) sections 8 of the Trademark Act
Criminal penalties for misuse of trademarks RCW 9.16.030 to .060
Applicable purchasing rules apply per Purchasing Services policy BPPM 70.01

AUDIT STANDARDS

Our office follows the guidelines as promulgated by the Institute of Internal Auditors’ “International Standards for the Professional Practice of Internal Auditing” (IIA Standards), in carrying out the planning and engagement of audit activity. The IIA Standards required we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we included such tests of the records and other procedures as we considered necessary in the circumstances.

The WSU Office of Internal Audit is not in full conformance with the IIA Standards in that a quality peer review has not yet been performed.

AUDIT TEAM INFORMATION

Internal auditors assigned to the audit include:

Lead Auditor  Jaya Sivakumar
Supervisor          Heather Lopez

For questions regarding this project, contact Heather Lopez, Chief Audit Executive:

Email:  hlopez@wsu.edu
Phone: (509) 335–2001
Website:  http://www.internalaudit.wsu.edu