Southern OREGON UNIVERSITY

OFFICE OF THE BOARD OF TRUSTEES

Public Meeting Notice

June 12, 2020

TO: Southern Oregon University Board of Trustees, Executive and Audit Committee

FROM: Sabrina Prud'homme, University Board Secretary

RE: Notice of Regular Meeting of the Executive and Audit Committee via Zoom

The Executive and Audit Committee of the Southern Oregon University Board of Trustees will hold a regular meeting on the date and at the location set forth below.

The topics of the meeting will include a report from the internal auditor and discussion and action on the internal audit plan for 2020-21. There also will be updates on cybersecurity and the governance work group.

The meeting will occur as follows:

Friday, June 19, 2020
10:30 a.m. to 11:30 a.m. (or until business is concluded)
Visit governance.sou.edu for meeting materials.
To join or view the proceedings, visit https://sou.zoom.us/j/91265695401 at the time of the meeting.

If special accommodations are required or to provide written public comment or testimony, please contact Kathy Park at (541) 552-8055 at least 72 hours in advance.

Public Comment
Members of the public who wish to provide public comments for the meeting are invited to submit their comments or testimony in writing. Please send written comments or testimony to the Board of Trustees email address: trustees@sou.edu. Public comments also may be sent to the board via postal mail addressed to SOU Board of Trustees, 1250 Siskiyou Boulevard, Ashland, OR 97520.

Board of Trustees
Executive and Audit Committee Meeting
June 19, 2020

Call to Order / Roll / Declaration of a Quorum

Board of Trustees
Executive and Audit Committee Meeting

Friday, June 19, 2020
10:30 a.m. – 11:30 a.m. (or until business concludes)
DeBoer Room, Hannon Library

AGENDA

Persons wishing to participate during the public comment period shall sign up at the meeting.
Please note: times are approximate and items may be taken out of order.

	1	**Call to Order/Roll/Declaration of a Quorum**	Chair Lyn Hennion
	1.1	Welcome and Opening Remarks	
	1.2	Roll and Declaration of a Quorum	Sabrina Prud'homme, SOU, Board Secretary
	1.3	Agenda Review	Chair Hennion
	2	**Public Comment**	
5 min.	**3**	**Consent Agenda**	
	3.1	Approval of April 21, 2020 Meeting Minutes	Chair Hennion
	4	**Reports**	
5 min.	4.1	Internal Audit Report	Ryan Schnobrich, SOU, Internal Auditor
	5	**Action, Information and Discussion Items**	
20 min.	5.1	Internal Audit Plan for 2020-21 (Action)	Ryan Schnobrich
20 min.	5.2	Update on Cybersecurity	Tom Battaglia, SOU, Chief Information Officer
5 min.	5.3	Governance Work Group Update	Vice Chair Paul Nicholson; Trustee Megan Davis Lightman
	5.4	Future Meetings	Chair Hennion
	6	**Adjournment**	Chair Hennion

Public Comment

Consent Agenda

Board of Trustees
Executive and Audit Committee Meeting
Tuesday, April 21, 2020

MINUTES

Call to Order/Roll/Declaration of a Quorum

Committee Members:

Lyn Hennion	Present	Paul Nicholson	Present
Sheila Clough	Present	Daniel Santos	Present
Megan Davis Lightman	Present	Bill Thorndike	Present

Chair Lyn Hennion called the meeting to order at 9:33 a.m. in the DeBoer Room of the Hannon Library. The secretary recorded the roll and a quorum was verified.

Other trustee in attendance: President Linda Schott, janelle wilson

Other attendees included: Greg Perkinson, Vice President for Finance and Administration; Jason Catz, General Counsel; Dr. Neil Woolf, Vice President for Enrollment Management and Student Affairs; Dr. Susan Walsh, Provost; Sabrina Prud'homme, Board Secretary; Ryan Schnobrich, Internal Auditor; Josh Lovern, Budget Office; and Kathy Park, Office of the Board Secretary.

Reports

Internal Audit Report

Taking agenda items out of order, Ryan Schnobrich provided the Internal Audit Report. He referred trustees to the meeting materials, noting the Recreation Management and Veterans Management Action Plans were completed since the committee's last meeting. Housing and Deferred Maintenance are nearing completion and progress is being made on Athletics, but COVID has significantly disrupted operations in these areas. The audit of the student fee process will be complete after the May board meeting. This year's annual assessments of management responsibility and fraud risk control are also delayed because of COVID. Mr. Schnobrich said President Schott asked him to assist the incident response team, which he has been able to do in a capacity that has not affected his independence or objectivity nor caused him to participate in management. To assist with budget savings, he decided not to hire a student employee and not to pursue a quality assurance review of Internal Audit next year.

With COVID and management's push to close out management action plans, Mr. Schnobrich said he delayed his services that had not already started or that would require management involvement in the short term. He was pleased to observe SOU's new Compliance Task Force discuss student accessibility during remote instruction and he is looking forward to discussing various privacy-related compliance requirements in the future.

Mr. Schnobrich said he cancelled the Oregon Equal Pay Act audit and will reconsider it for next year based on the vice presidents' risk assessment and related feedback as they discuss next year's internal audit plan. There are many risk topics to consider and limited resources to engage, especially given the ongoing disruption to operations. Responding to Chair Hennion's and Trustee Santos' inquiries, Mr. Schnobrich described

his contributions on COVID-related issues and risks.

Responding to Trustee Sheila Clough's inquiry regarding the impact of putting audits and tasks on hold, Mr. Schnobrich said it is a matter of coverage and limited management compliance resources to engage on these topics. Although there is not as much coverage as desired, this does not pose a specific risk. Anti-fraud initiatives related to COVID fall under Business Services and he is assisting with those initiatives; this, however, does not stop management's anti-fraud efforts to mitigate risks, such as IT's cybersecurity program and the additional discipline and proposed organizational changes in Business Services.

Public Comment
There was no public comment.

Consent Agenda
Vice Chair Paul Nicholson moved to approve the consent agenda, as presented. Trustee Clough seconded the motion and it passed unanimously.

Action, Information and Discussion Items
Board Elections Process (Action)
Jason Catz reviewed the key elements of the proposed board elections process. There will be a work group of 3-5 trustees tasked with receiving and reviewing recommendations for the chair and vice chair positions. Included on the work group will be one past-chair or vice chair and at least one of the trustees who serves by virtue of their position as a student, staff or faculty. Trustees cannot serve on the work group if they intend to be nominated, recommend themselves, or would accept a recommendation; trustees would have to recuse themselves if that situation arose. The work group would review all recommendations and those recommended for the positions would be asked to submit a statement of interest. After reviewing the statements of interest, the work group may ask for additional information from the candidates. There will be an opportunity for the work group chair or designee to discuss concerns about any of the candidates. Candidates can withdraw at any time in the process. At the board meeting, all candidates will be discussed and nominated, at which point there will be a vote. The nominee receiving a majority of the votes will occupy the chair position. If no nominee receives a majority of votes, the top two would go through a run off and the person receiving a majority of votes would prevail. For those candidates interested in the vice chair position, the process would repeat itself.

Chair Hennion said the terms for the chair and vice chair would be two years. Mr. Catz, Sabrina Prud'homme and Trustee Megan Lightman said they thought two-year terms would be beneficial for the board.

Responding to Chair Hennion's comment, Ms. Prud'homme said that, despite the late date, the elections process could still be completed in 2020 but would be compressed. Having fewer trustees on the work group would allow the group to be more nimble in scheduling meetings and would accomplish the process more expeditiously.

Discussion ensued on the legal limits on trustees' terms and the impact of that limitation on a trustee serving a two-year term as a chair or vice chair. The consensus was to have the Board Statement remain silent on the topic at this time, which would

provide the board flexibility and would not be overly constraining.

At Vice Chair Nicholson's request, President Schott provided input on the proposed process and her role in it, saying she is comfortable with the process but it is one the trustees need to feel comfortable with. She has good relationships with all of the trustees so it would be an easy transition to whomever becomes the chair. Mr. Catz added that there is language in the statement about the work group consulting with the president.

Trustee Bill Thorndike moved to accept the Board Statement on the Process for Officer Elections as presented. Trustee Santos seconded the motion and it passed unanimously.

Review of Authorities and Related Communication

Chair Hennion said this is a review item on the agenda just to remind trustees of the delegated versus retained authorities, and those which the board cannot delegate. Given the guidelines SOU must follow, which are changing on almost a daily basis during the COVID crisis, SOU must be able to remain nimble in order to manage the university and best serve students in compliance with state and federal laws.

It is important to remember that the Executive and Audit Committee has the authority to act on behalf of the board, but in case a quorum cannot be assembled in an emergent situation, the president may need to act in order to support the needs of students or the university. During this pandemic, this is precisely the time the president may need to rely on certain powers. The Board Statement on Delegation of Authority provides for this already, but it is important that the committee reminds itself of these authorities as well as expected communication in this area.

Mr. Catz said it is evident how emergent the current situation has been in terms of public health and safety issues and economic impacts. He referred to paragraph 2.3 of the Delegation of Authority which authorizes the president to take emergency and temporary actions when necessary, emphasizing invocation of this provision must be both emergent and temporary. President Schott added her appreciation that this provision is already included in the board's documents. If there is a case when she needs to act quickly, she does not need special action to do so, which would avoid causing unnecessary concern.

Future Meetings

Chair Hennion said the next committee meeting will be on June 19.

Adjournment

Chair Hennion adjourned the meeting at 10:21 a.m.

Internal Audit Report

Southern Oregon University
Internal Audit Annual Report
Fiscal Year 2020

Prepared By
Ryan Schnobrich, C.P.A., C.I.A.
Internal Auditor

June 19, 2020

TABLE OF CONTENTS

Introduction

This report outlines the Internal Auditor's accomplishment of the Fiscal Year 2020 Internal Audit Plan.

As reported in April's Executive & Audit Committee meeting, the Covid-19 pandemic has caused considerable operational and financial disruption beginning March 13, 2020. Any Internal Audit services that did not directly assist management were stopped. Internal Audit took FEMA emergency operations training and joined the university's Incident Response Team in a consulting capacity. Being that everyone immediately began working from home, participating in the Incident Response Team continues to be a good way for all the resulting changes and evolving risks to be visible to Internal Audit.

Turnover and vacancy in key collaborator positions continued to affect management compliance and momentum on completing this year's Internal Audit Plan. These positions were, or currently are, either vacant, frozen, eliminated or filled by interim administrators whom, not only already have full-time positions, but also are 20% furloughed like the Internal Auditor and the rest of the management and senior staff with whom Internal Audit integrates:

- Chief Diversity & Inclusivity Officer
- Title IX Coordinator;
- Women's Resource Center Coordinator;
- Director of Campus Public Safety;
- Financial Aid Compliance Officer;
- Service Center Quality Control/Compliance Coordinator;
- Financial Analyst

Assurance Services	Comment	Status
Facilities Management & Planning – Sustainability Reporting to AASHE		Completed – 8/19/2019
Campus Public Safety – Re-perform FY17 stopped audit of Clery Act compliance		Completed – 10/14/2019
ASSOU – Reperform FY17 stopped audit of Student Fee Process - ORS 352.105	Process completed at May 22, 2020 Board Meeting.	Final testing and drafting of the report will be completed in FY21
Annual Assessment of Management Responsibilities	The assessment is complete.	The report is posted on Internal Audit's Board reporting website.
Annual Assessment of Management's Control of Fraud Risk	The assessment is complete.	The report is posted on Internal Audit's Board reporting website.

Human Resources - Oregon Equal Pay Act compliance	Cancelled due to Covid-19.	Pre-audit process/internal control walkthrough showed low likelihood of a risk event.
Miscellaneous as requested by management	No significant requests this year.	

Consulting Services	**Comment**	**Status**
VP F&A – Culture of Continuous Improvement, Assessment/Analysis & Accountability	Service Excellence initiative. Ethics, Culture & Accountability discussions. Continuous Improvement Facilitator Committee.	Will continue in FY21.
VP EMSA – Scholarships assessment	Revenue management principles implemented. New scholarship portal.	Completed – 12/30/2019
VP EMSA – Student Record Maintenance	Gramm-Leach-Bliley Act risk assessment completed with CIO, Registrar & Director of Financial Aid.	Scope broadened and will continue in FY21.
Financial Aid - Internal controls around key processes, compliance requirements and enhancement of enterprise risk management	Financial Aid Compliance Officer position vacated and not filled.	Stopped – 2/3/2020
Business Services Payroll – Integrative processes;	Some policies rewritten. Processes streamlined, better integrated, better controlled, escheat completed.	Completed – 12/19/2019
Facilities Management and Planning – Surplus assets process	Process improvement walkthrough. Policy reviewed.	Completed – 1/7/2020
Follow Up - Selected Oregon University System Internal Audit Division audit recommendations		Internal Audit will resurface prior recommendations as new observations warrant.
Follow Up - FY17 Title IX audit management response and action plan	Campus Climate Survey completed. Organizational changes ongoing. Title IX Regulations recently changed.	Clery, Title IX and VAWA continue to be an area worthy of Internal Audit's attention.
Follow Up - FY17 investigation report	Completed management response and action plans	Housing's management response and action plan will

management response and action plan(s)	reported to the Board of Trustees.	continue in FY21.
Follow Up – FY18 stopped audit regarding Irregular Employment Agreements;	Process improvement facilitator and executive champion identified.	Will continue in FY21.
Follow Up – FY18 investigation report management response and action plan(s);	Completed management response and action plans reported to the Board of Trustees.	Facilities' is completed. Housing's is not. Reporting to the Board will occur in FY21.
Follow Up – FY19 investigation report management response and action plan(s)	The relevant members of management are actively working the plan.	Will continue in FY21.
Miscellaneous as requested by management;	In March, President Schott requested that I participate on the Incident Response Team led by VPF&A.	Will continue in FY21.

Internal Control Assessments	Comment	Status
Business Services – Pcard Administration	Pcard policy rewritten and trained upon. Duties and responsibilities reorganized. Internal controls improved as well as flexibility – especially in Athletics.	Completed – 5/27/2020
Business Services – Journal Entries, Reserve Balances, Anti-Fraud Initiatives, Banner 9 Access & Security, Vendor Maintenance, Travel, Grants	Associate Director of Business Services hired. Duties and responsibilities reorganized including the Service Center.	Department reorganization and Covid-19 disruption necessitate moving these topics to the FY21 Internal Audit plan as ERM consulting.
Gramm-Leach-Bliley Act (Cybersecurity/Financial Aid)		Completed – 1/15/2020
Cultural Competency Compliance		Completed – 1/24/2020
Vehicle Use	Provided management with feedback regarding driver clearance and the van pool.	Completed – 3/9/2020

Investigative Services & Coordination with Management's Compliance Function

I opened thirteen new allegations last fiscal year and finalized almost all open investigations. None of the closed investigations rose to the level of providing a report to the Board of Trustees. I appreciate how management has been working through the myriad of topics.

Management's compliance function is primarily embedded in management and coordinated by committee. I am a contributing guest at:

- Vice President of Finance & Administration's Business Affairs Council
- General Counsel's Policy Council
- Director of Environmental Health & Safety's Occupational Safety Advisory Council
- ASSOU's Student Recreation Center Advisory Council

Coordination with External Auditors

Each year, as part of the single audit, our external auditors, CliftonLarsonAllen, interview me regarding management's internal control structure and progress in implementing enterprise risk management. We review and discuss my reports to the Board of Trustees in confidence.

Risk Assessment

As I become aware of them, I continue to note key risks, key internal controls by risk type and greatest opportunities in a risk and control matrix. Please see the Internal Audit Plan for FY21 and this year's Annual Assessments for more information.

Governance, Risk Management and Control

I have become more familiar with universities' governance, risk management and compliance functions.

- I have recurring one-on-one meetings with the Chair of the Board of Trustees, the President, the General Counsel, the Vice President of Finance and Administration, the Board Secretary and the Director of Human Resources.
- I attended all Board meetings prior to Covid-19, but needed to miss some in March and April due to an illness in my family.
- All conferences and most meetings with the other public higher education Chief Audit Executives were cancelled this year due to cost savings and/or Covid-19.

Department Procedures, the *Standards* and the Quality Assurance Improvement Program

As reported in the April Board meeting, to save approximately $5,000, the decision has been made to not perform a peer external quality assurance review for FY21. Internal assessments and self-monitoring are ongoing, but future reports to the Board will indicate noncompliance with the *Standards* in this regard.

I believe that my involvement added value to campus operations and governance.

Internal Audit consistently returns budget savings to the Office of the President each year – this year amounted to more than $9,000. This was accomplished these last two years primarily by cancelling nearly all travel and training, and holding a student-worker position open. Unfortunately, I must attend the next two national Association of College and University Auditors conferences or risk nonrenewal of my Certified Public Accountant license.

Annual Confirmation of the Organizational Independence of Internal Audit

Management did not interfere in determining the scope of internal auditing, control which areas I examined, or what information I communicated. All determinations and work were performed independent from management decision-making. I did not subordinate my judgment on audit matters to others.

Exhibit A

Annual Required Communication with the Executive & Audit Committee Checklist

Standard	Communication Requirement	Annual Communication Documentation
1000	The Chief Audit Executive (CAE) must periodically review the Internal Audit Charter and present it to senior management and the Audit Committee for approval.	The SOU Internal Audit Charter was updated for IPPF 2017, reviewed with executive management and then presented to the Executive and Audit Committee for review and approval at the January 16, 2018 committee meeting.
1010	The CAE should discuss the Definition of Internal Auditing, the Code of Ethics, and the IIA *Standards* with Senior Management and the Finance and Audit Committee.	The Definition of Internal Auditing, the Code of Ethics, and the *Standards* were discussed with executive management and the Executive and Audit Committee in conjunction with the revision of the SOU Internal Audit Charter at the January 16, 2018 committee meeting.
1110	The CAE must confirm to the Executive and Audit Committee, at least annually, the organizational independence of the internal auditing activity.	By reporting functionally to the Executive & Audit Committee and administratively to the President, the Internal Auditor confirms the organizational independence of the internal audit activity as of June 19, 2020.
1111	The CAE must communicate and interact directly with the Executive and Audit Committee.	As the Chief Audit Executive, I confirm that an appropriate level of communication and interaction has taken place between me and the Executive and Audit Committee during FY20.
1112	The CAE's independence and objectivity may be impaired if the CAE is asked to perform roles for which management is normally responsible. This could include risk management, design and operation of internal controls and compliance.	The CAE did not have operational responsibilities in FY20.
1120	Internal Auditors must have an impartial, unbiased attitude and avoid any conflict of interest.	The CAE certifies his impartiality and unbiased attitude in FY20. The CAE has avoided any conflict of interest in FY20.
1130	The CAE must disclose the details of any impairment to independence or objectivity, whether in fact or appearance.	The CAE did not have impairment of independence or objectivity in FY20. There was no self-interest, self-review, familiarity, bias, or undue influence. There were no personal conflicts of interest, scope limitations, resource limitations, restrictions on access to records, personnel or property. Results or approaches were not modified.

		There were two minor but related incidents where consulting work I performed for President Schott regarding House Bill 4141 (tuition setting) was inaccurately communicated as my having provided assurance, first to the Higher Education Coordinating Commission in FY19 and then again as part of May 2020's Board of Trustees reporting package. It is not believed that this affected decision-making in any way, but if assurance doesn't come directly from me, it is false assurance. Like an attorney or doctor, management may not speak my voice. It is believed to have been unintentional then followed by a transcription/duplication error, but if it were to continue, it could be considered a threat to the independence of Internal Audit.
1200	Engagements must be performed with proficiency and due professional care.	The CAE developed the necessary knowledge, skills and competencies to perform FY20 Internal Audit Plan via education, experience, professional development, interview and research of experts and colleagues, maintaining and acquiring of professional certifications, participation with ACUA, IIA and AICPA and understanding of and adherence to the *Standards'* systematic and disciplined approach to internal auditing. Policies and Procedures are adhered to and are continuously improved.
1300	The CAE must develop and maintain a quality assurance and improvement program (QAIP) that covers all aspects of the internal audit activity.	The CAE has a thorough understanding of the mandatory elements of the IPPF (the *Standards* and IIA Code of Ethics). In FY18, the CAE read the IIA's *"Quality Assessment Manual for the Internal Audit Activity"*. I believe that the internal audit activity is in compliance with the *Standards* and that the IIA Code of Ethics is applied. Drafting and improving of policies and procedures are ongoing.
1311	The CAE is responsible for ensuring that the internal audit activity conducts an internal assessment that includes both ongoing monitoring and period self-assessments.	A self-assessment has not been performed because it would need to be validated by a qualified, independent, competent, and professional external assessor to be valid. Internal assessments, standardization of work practices and self-monitoring are ongoing. An audit quality assurance template was created in FY18.
1312	The CAE must discuss with the Executive and Audit Committee the form and frequency of external assessment as well as the qualifications and independence of the external assessor or assessment team, including any potential conflicts of interest.	The Executive & Audit Committee was advised on June 17, 2016 that a Quality Assurance Review (QAR) must be performed every five years. The Chief Audit Executives of the other Oregon public higher education institutions have offered to complete the QAR when there is sufficient material to review (FY21). The Board was advised on April 21, 2020 that due to budgetary reasons it has been decided to not go forward with the Quality Assurance Review.

1320	The CAE must communicate the results of the quality assurance and improvement program to senior management and the Executive and Audit Committee. The results of external and periodic internal assessments are communicated upon completion of such assessments and the results of ongoing monitoring are communicated at least annually. The results include the reviewer's or review team's assessment with respect to the degree of conformance.	Establishing a Quality Assurance Improvement Program (QAIP) including developing and performing a client survey was completed as part of the FY17 Internal Audit Plan. Further development of a QAIP was completed in FY18, FY19 and FY20.
2000	The CAE must effectively manage the internal audit activity to ensure it adds value to the organization.	The CAE meets with executive management and the Board to obtain an understanding of the university's strategies, objectives, associated risks and risk management processes. The CAE has attentively followed the President's strategic planning process in FY18 & FY19.
2010	The CAE must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.	The CAE meets with the President (May 7th and June 2nd 2020) and Vice Presidents (February 25th) each fiscal year to discuss the university's key objectives and associated risks to seek input into the annual Internal Audit Plan. Business Affairs Council discussed risks at least monthly during FY20 and the VPF&A presented to the Board on January 16th 2020.
2020	The CAE must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the Executive and Audit Committee for review and approval. The CAE must also communicate the impact of resource limitations.	Communication of the status of internal audit plans and resource requirements was reported to the Executive & Audit Committee on October 18th 2019, January 17th and April 21st 2020. Significant interim changes were communicated to and approved by the Board on April 21st 2020.
2030	The CAE must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.	Although modest, and because the Board of Trustees has been accepting of the Internal Audit Plan being reduced at times, the CAE believes that resources are appropriate and sufficient. There have been no inappropriate reductions in resources or restriction of activities. No external expertise has been utilized or is expected to be utilized at this time. The Internal Audit Plan for next year is not as ambitious due to Covid-19 social distancing and 20% furloughs.
2040	The CAE must establish policies and procedures to guide the internal audit activity.	The CAE drafted numerous policies and procedures in FY17. They were reviewed, revised and added to in FY18. There was some ongoing drafting and revising of policies and procedures in FY19 and FY20.
2050	The CAE should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.	The CAE reads the audit reports for the university's single audit each fiscal year. Please see the annual assessment of management's responsibilities and control of fraud risk. The Financial Aid Compliance Coordinator position was eliminated by management.
2060	The CAE must report periodically to senior management and the Executive and Audit Committee on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the Audit Committee.	Communication of IA's purpose, authority, and responsibility was explained during new Trustee onboarding in FY18, FY19 and FY20. Significant risk exposures and control issues including fraud risks, governance issues and other matters are reported quarterly to the Executive & Audit Committee. The CAE meets regularly with the President, VP of F&A, General Counsel, Board Secretary and Chair of the Board of Trustees.

2100	The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach.	The CAE has reviewed the university's mission, key objectives, critical risks, and the key controls used to mitigate such risks. Please see the annual assessment of management's responsibilities regarding governance, risk management, and internal control activities. Please see the annual assessment of management's control of fraud risk.
2110	The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for…	Please see the annual assessment of management's responsibilities regarding governance activities.
2120	The CAE must evaluate the effectiveness and contribute to the improvement of risk management processes.	The CAE completes annual assessments of management's responsibilities and management's control of fraud risk. FY18 Consulting included guiding enterprise risk management in IT. Financial Aid's COSO ERM requirement was communicated to management and the Board in FY17 & FY18 annual reports. The VPF&A reported enterprise risk management progress to the Board in FY19 and FY20. Please see SOU risk management timeline in both FY20 and FY21 Internal Audit Plans.
2130	The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.	Please see the annual assessment of management's responsibilities regarding internal control activities. Please see the annual assessment of management's control of fraud risk. A comprehensive risk and control matrix was created in FY17. This model is updated as information becomes available or observed, but "boiling the ocean of risk" is no longer a best practice.
2200	Internal Auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.	An engagement plan is created for each audit and consulting engagement. An engagement plan is created for investigations when it is believed that there will be a report to the Board or when performing work under attorney-client privilege.
2600	When the CAE concludes that management has accepted a level of risk that may be unacceptable to the organization, the CAE must discuss the matter with senior management. If the CAE determines that the matter has not been resolved, the CAE must communicate the matter to the Board.	The CAE and the Chair of the Board of Trustees, President, Vice President of Finance & Administration, General Counsel and Board Secretary have regular one-on-one meetings. The CAE has not felt compelled to advise the Board on any unacceptable acceptance of risk by senior management, but it should be noted that, in the CAE's opinion, the Board has accepted a degree of risk without my assurance of compliance in regards to the Clery Act/VAWA.

Internal Audit Plan for 2020-21 (Action)

Southern Oregon University
Internal Audit Plan
Fiscal Year 2021

Prepared By
Ryan Schnobrich, C.P.A., C.I.A.
Internal Auditor

June 19, 2020

TABLE OF CONTENTS

Introduction & Internal Audit Plan Overview

The purpose of the Internal Audit Plan is to outline services and activities the Internal Audit Department will conduct during Fiscal Year 2021. The Internal Audit Plan satisfies responsibilities established by the Board of Trustees bylaws, the Internal Audit Charter, and applicable professional *Standards*. The Internal Audit Plan should be based on appropriate risk-based methodology, including the consideration of any risks or control concerns identified by management.

The Internal Auditor is authorized to make changes to the Internal Audit Plan, as deemed necessary, to address changes in identified risks. The Executive and Audit Committee and the President will be notified of any significant additions, deletions, or other changes to the Internal Audit Plan.

Executive Summary

Please refer to Internal Audit's annual report, annual assessments of management responsibilities and management control of fraud risk, engagement reports and reference resources on the Board reporting page:

https://sites.google.com/a/sou.edu/internal-audit/filecabinet

Several key collaborators, namely the Chief Diversity and Inclusivity Officer, Title IX Coordinator, and Director of Campus Public Safety, are being filled in the interim by colleagues that not only already have full-time positions, but also are 20% furloughed like the Internal Auditor and the rest of the management and senior staff with whom Internal Audit integrates. Other positions, such as the Financial Analyst and the Financial Aid Compliance Officer have been eliminated after their vacancy due to budget cuts.

This year's internal audit plan primarily focuses on

- being available as an assurance and consulting resource to management especially including supporting the Finance Section of the Incident Response Team;
- increasing management engagement in topics explored in Internal Audit's annual assessments of management responsibility and fraud risk control;

Internal Audit Risk Assessment Overview

"The internal audit activity, as an independent assurance function, performs engagements to assess that risk management processes are effective in individual areas and overall throughout the entire organization. Additionally, the internal audit activity may compare its risk assessments to the risk information produced by management and verified by the internal assurance functions (compliance/risk management) to gauge the accuracy and completeness of management's assessment. Conversely, the internal audit activity may use management's risk information to inform internal audit's risk assessments, or they may do both as appropriate. The Chief Audit Executive should coordinate with other providers of assurance and consulting services and may consider relying on their work (Standard 2050 – Coordination and Reliance)."

The Vice Presidents' risk assessment input and experiencing several risk events, namely the pandemic and financial going concern, factored significantly in what was included in this year's internal audit plan. Given the mutual effort this past year, Internal Audit relied considerably on managements' risk assessment for this next year's internal audit plan. Internal Audit encourages the Vice Presidents to perform both high-level and broad-based risk assessment across all operations throughout next fiscal year.

Internal Audit Plan for Fiscal Year 2021

Assurance/Audit Services:

1. Associated Students of Southern Oregon University – The Student Fee Process and administrative compliance with ORS 352.105 (Mandatory Incidental Fees);
    a. This audit is complete pending final testing and drafting of the report.
2. Office of the Vice President of Finance & Administration – Document completion of FY16 & FY17 Management Response and Action Plans and reports to the Board of Trustees;
3. Annual Assessment of Management Responsibilities;
4. Annual Assessment of Management's Control of Fraud Risk;
5. Miscellaneous as requested by President Schott, which may include auditing our FEMA submission, use of CARES Act funds, or similar;

Consulting Services:

1. Office of the Vice President of Finance & Administration – Incident Response Team;
2. Director of Budget & Planning - President's Council on Financial Sustainability;
3. (Associate) Director of Business Services – Enhancement of Enterprise Risk Management;
4. Office of the Vice President of Finance & Administration – Continuous Process Improvement, Assessment/Analysis, Ethics, Accountability and Cultural Change;
5. Office of the Vice President of Enrollment Services & Student Affairs – Student Information Privacy Compliance

6. Office of the President with the General Counsel and new Title IX Coordinator – FY17 Title IX audit management response and action plan;
7. Office of the Vice President of Finance & Administration via the Director of Human Resources – FY18 stopped audit regarding Irregular Employment Agreements;
8. Office of the President with the General Counsel and new Title IX Coordinator – FY19 Clery Act and Violence Against Women Act audit management response and action plan;
9. Office of the President via the Director of Athletics and General Counsel – Open FY19 Investigation Management Action Plan;

Investigative Services:

1. EthicsPoint hotline allegations come to me for substantiation and reintegration with management decision-making.
2. Internal Audit coordinates with other functions that perform investigations.

Governance:

1. Continue to develop an understanding of the Board of Trustees and management's risk appetite in the context of the next phase of the strategic plan.
2. Continue to be a contributing guest at Business Affairs Council, Policy Council and the Organizational Safety and Compliance Committee.

Risk Assessment:

1. Encouraging management risk assessment and enterprise risk management;
2. Nurturing a formal compliance management function by management;
3. Continued harvesting of risk and controls and entering them into a risk matrix.

Internal Control Assessment:

1. Miscellaneous as requested by management.

Annual Confirmation of the Organizational Independence of Internal Audit

Another key responsibility set forth in the Internal Audit Charter is to confirm annually the organizational independence of Internal Audit. This is included in each year's Internal Audit Plan. The Board will be advised of any responsibilities or conditions believed to affect the objectivity or independence of Internal Audit, as well as any limitations to scope or insufficient resources to perform internal audit services.

Human Resource Plan

The Fiscal Year 2021 Internal Audit Plan was created around the understanding of having one Internal Auditor on 20% furlough and Internal Audit's student employee position left vacant for a second year to generate budget savings.

Any Resource Limitations or Significant Interim Changes

Having only one Internal Auditor is inherently a resource limitation so being 20% furloughed like all the members of management Internal Audit integrates with, that were already capacity constrained, is a significant resource constriction for which the Board of Trustees should manage expectations.

Financial Budget

As per the Internal Audit Charter, the Executive and Audit Committee is responsible for approving the internal audit function's budget and resource plan. Internal Audit's requested budget has been submitted to the Director of Budget & Planning.

In Fiscal Year 2020, Internal Audit skipped two conferences, curtailed travel and controlled costs to return more than $9,000 of budgeted expenses.

In Fiscal Year 2021, the Internal Auditor must attend the Association of College and University Auditors conference or risk being unable to renew his Certified Public Accountant license.

Appendix A
Risk Assessment Timeline

Stage	Culture	Governance	Process
1 – Initial	Risk belongs to the internal audit activity.	CAE/audit committee chair.	Risk-based auditing.
2 – Repeatable	Risk is considered on an as-needed basis.	Business managers.	As-needed risk and control self-assessment process.
3 – Defined	Risk information is shared among internal audit and control functions.	C-suite/board members.	Common risk language and risk assessment process are used by internal audit and control functions.
4 – Managed	Risk is integrated into strategic planning; risk appetite is stated and communicated.	All levels of management and the board.	Common risk language and consistent risk assessment process are in place throughout organization.
5 – Optimized	Risk is integrated into all decision-making, compensation, and goals.	Total participation.	Common risk language and aggregated risk reporting are established throughout organization.

Standard 2120 – Risk Management states, "The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes." Specifically, the standard requires the internal audit activity to assess whether:

1. The organization's objectives align with its mission.
2. Management assesses significant risks.
3. Management's risk responses align risks with the organization's risk appetite.
4. Relevant risk information is captured and communicated timely throughout the organization, including to the Board of Trustees.

In FY16, the Internal Audit department was formed. Internal Audit performed risk interviews with management that resulted in a list of the university's top ten risk areas (a "top down approach"), which was presented to the Board of Trustees.

In FY17, Internal Audit performed risk assessment procedures including management interviews and harvesting risks and their related internal controls into a matrix. Risk scoring criteria was developed, performed and recorded into the matrix (a "bottom up approach"). This information was summarized and presented to the Board in a heat map format. The heat map represented specific residual risks that could result in a material event if related internal controls were not implemented and functioning effectively.

At the end of FY17, per "Assessing the Risk Management Process" a practice guide from the Institute of Internal Auditors, we would appear to have achieved "initial – stage 1" maturity:

"In organizations where the risk management process is in early stages of development, the internal audit activity may be more actively involved than it would be when the process is more mature. At this maturity level, specific risk management activities may not be performed by the line/operational management or functions in the roles of control, compliance, legal, risk management, or internal quality assurance. Instead, those functions may rely on the internal audit activity's risk assessments and risk-based assurance and advice."

In FY18, at Internal Audit's urging, the Vice Presidents and Business Affairs Council performed high-level, "top down", risk assessments. Internal Audit assisted by attending risk assessment meetings and incorporating a heat map into management's tracking spreadsheet. Internal Audit and the Vice Presidents discussed their risk assessment.

At the end of FY18, we would appear to have achieved "repeatable – stage 2" maturity:

"At this level, the internal audit activity is better organized and resourced and plays an instrumental role by performing risk-based assessments, perhaps larger in scope. The internal audit activity may work with the control, compliance, legal, risk management, and internal quality assurance functions, adding internal audit expertise to assist risk owners in line/operational management functions to build and monitor operational controls. This stage is sufficient for many organizations if the process is operating consistently, efficiently, and delivering actionable results that aid in the attainment of the organization's goals and objectives."

In FY19 and FY20, the Vice Presidents, and especially the Business Affairs Council, independently performed broad-based "bottom up" risk assessment with Internal Audit's encouragement. The Vice President of Finance & Administration presented their combined risk assessment and heat map to the Board of Trustees on March 21, 2019. Internal Audit independently monitored and harvested internal and external risks and recorded it into its matrix.

At the end of FY19 and FY20 we would appear to be striving for "defined – stage 3" maturity:

"Organizations that rank toward the middle of the model may be a blend of maturity levels, with some business units operating at higher levels of maturity than others. In this structure, the organization's control, compliance, legal, risk management, and internal quality assurance functions may own the risk management process and have responsibilities that remain consistently within the Managed and Optimized levels, for example. The control and assurance functions may play an active role in assisting line/operational management to assess risks and perform other risk management activities. The internal audit activity may continue to operate functionally at the Repeatable level."

Southern Oregon University
Board of Trustees
Executive and Audit Committee

Resolution
Recommendation to Adopt Fiscal Year 2020-2021 Internal Audit Plan

Whereas, Southern Oregon University is governed by and the business and affairs of the University are managed by the Board of Trustees of Southern Oregon University;

Whereas, Southern Oregon University has a duty to responsibly manage, invest, allocate, and spend its resources;

Whereas, Southern Oregon University has created the position of Internal Auditor to provide independent and objective assurance, consulting and investigative services that add value to the University;

Whereas, the Board of Trustees of Southern Oregon University has granted the Internal Auditor an Internal Audit Charter ("Internal Audit Charter") to provide guiding principles, direction and authority to the Internal Auditor consistent with The Institute of Internal Auditors' International Professional Practices Framework; and

Whereas, the Internal Auditor will work closely with the Board of Trustees, University leadership, faculty and staff to conduct and coordinate a broad range of internal audit functions for the University; and

Whereas, the Internal Auditor has developed, for approval by the Board, a risk-based annual internal audit plan ("Internal Audit Plan") for Fiscal Year 2021, which the Executive and Audit Committee has reviewed; Now therefore,

Be it resolved, the Executive and Audit Committee hereby recommends the Board of Trustees of Southern Oregon University approve and adopt the Fiscal Year 2021 Internal Audit Plan. The committee further recommends that the Board instruct the Internal Auditor and the officers of the university to take all actions and steps deemed necessary and proper to implement the Internal Audit Charter and the Internal Audit Plan.

VOTE:
DATE: June 19, 2020

Recorded by the University Secretary:

_____

Update on Cybersecurity

(This section updated)

2020 Cybersecurity Risk Assessment & Updates

Executive Summary

In 2019, SOU Information Technology responded to an audit of Gramm-Leach-Bliley-Act compliance, covering three broad areas (CliftonLarsenAllon, November, 2018):

1. Verify that the Institution of Higher-Education (IHE) has designated an individual to coordinate the information security program
2. Obtain the IHE risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b)
3. Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk

At the time of this request, SOU had designated that an Information Security Officer (ISO) had been identified, and a formal written position description had been submitted to and recorded by HR. In addition, as of late October 2019, a written information security program was completed based on the Center for Internet Security's CIS-20 framework. However audit criteria numbers two and three had not been completed.

SOU's CIO and ISO looked to Educause (a national association of IHE I.T. organizations) and consulted other large universities (UO, UW) for risk-assessment templates. Working with SOU's Internal Auditor, it was determined that neither the Educause nor the UO risk assessments actually evaluated risk-- they only assessed maturity of controls. Thus SOU devised a thorough risk assessment that evaluates the contributors to risk in a manner that can be scored. SOU's framework is based on the CIS-20 set of controls, but it augments the controls to calculate the risk exposed at SOU in each area. The methodology for the risk assessment is included.

SOU has performed this risk assessment twice. The first was conducted in November of 2019 and the second in June of 2020. Results are combined to identify areas of improvement or areas where the risk may have increased.

With the huge shift to remote delivery and remote work in 2020, it was important to maintain objectivity and honesty about the actual risks at the point in time. Thus, the results do demonstrate an increase of risk in some areas. This is largely due to the increase in entropy that occurred when shifting the workforce to working remotely.

For example, the ability to control the inventory of software assets decreased with working remotely. Contrarily, the reduced number of people on site and the locked buildings actually

decreased the likelihood that unauthorized devices would connect to the network, resulting in an improved risk score.

The area where the risk increased the most was incident response and management. This was due to an over-inflated sense of our maturity in this area. Through the first incidents that occurred in late 2018 and early 2019, visibility into incident response and management was restricted to I.T. The initial responses were string. Later in 2019 several other incidents occurred outside of I.T. SOU was fortunate that two of these cases were brought to the attention of the CIO and ISO; however, it also raised the concern for how thorough all of SOU's employees behave when security incidents occur.

Additional Updates

Awareness and Training

In accordance with the CIS-20 as well as required by the GLBA, an information security awareness and training program was established. This training has been designed to raise SOU's employees awareness of phishing attacks.

- Three formal simulated phishing campaigns were conducted over the past year. (See additional document, "Cybersecurity Hot-sheet Feb. 2020."
- A mandatory training program comprising four relevant videos began in May. To date, 34% of SOU employees have completed this training.

Storage, Backup & Recovery, Logging and Audit

SOU has embarked on the implementation of Box.com as its enterprise storage solution. Box has received the highest ratings in the space for security and functionality.

- Box.com manages backups and recovery for SOU, reducing risk.
- SOU added the Box Governance module that provides audit and logging of all file transactions. This is a huge improvement over the past system.

Vulnerability Detection

SOU has taken advantage of an offer extended through OHSU for an expanded version of the vulnerability tools that were being used.

Account Management and Boundary Defense

SOU has gained ground towards its management of accounts, access and its boundary defense.

- The most significant change is the rollout of mandatory multi-factor-authentication (MFA) using DUO.

- SOU eliminated its VPN connection to OSU, reducing the number of attackable nodes by the number of ports on OSU's campus.

Penetration Testing

Formalized, third-party penetration testing is recommended and even required by some regulations.

- The limitation has been financial and time restrictions.
- This is the next area that needs to be addressed.

2020 SOU Risk Summary Report Fiscal Year End

			Unmitigated Risk		
			2019	2020	Change
CIS Control 1:	**Inventory and Control of Hardware Assets**		81	54	**(27.0)**
CIS Control 2:	**Inventory and Control of Software Assets**		120	140	20.0
CIS Control 3:	**Continuous Vulnerability Management**		108	108	
CIS Control 4:	**Controlled Use of Administrative Privileges**		104	78	**(26.0)**
CIS Control 5:	**Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**		51	51	
CIS Control 6:	**Maintenance, Monitoring and Analysis of Audit Logs**		147	147	
CIS Control 7:	**Email and Web Browser Protections**		49	49	
CIS Control 8:	**Malware Defenses**		106	106	
CIS Control 9:	**Limitation and Control of Network Ports, Protocols, and Services**		106	84.8	**(21.2)**
CIS Control 10:	**Data Recovery Capabilities**		129	129	
CIS Control 11:	**Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches**		86	86	
CIS Control 12:	**Boundary Defense**		100	75	**(25.0)**
CIS Control 13:	**Data Protection**		81	94.5	13.5
CIS Control 14:	**Controlled Access Based on the Need to Know**		36	36	
CIS Control 15:	**Wireless Access Control**		96	76.8	**(19.2)**
CIS Control 16:	**Account Monitoring and Control**		36	36	
CIS Control 17:	**Implement a Security Awarness and Training Proogram**		144	72	**(72.0)**
CIS Control 18:	**Appplication Software Security**		138	92	**(46.0)**
CIS Control 19:	**Incident Response and Management**		103	206	103.0
CIS Control 20:	**Penetration Tests and Red Team Exercises**		144	144	

This summary illustrates the changes in risk between November, 2019 and June, 2020. Negative scores are shown in parentheses and reflect reduction in risk. Positive scores reflect increases in risk.

SOU Risk Assessment Approach

Methodology

Modes of Impact

We have identified four modes of impact for the consequences associated with risk to the University:

Direct Financial

Operational

Reputational

Human Safety

The modes are inter-related. For example, operational deficiencies are likely to impact finances, reputation, and possibly human safety at the University.

All risk is understood to have at least an indirect financial impact.

To faciliate comparison and prioritization, impact is expressed solely in financial terms in this assessment.

Financial Impact

Rating	Cost Range	Cost Range Expressed as Power of 10
3	$1 - $9,999	10^3
4	$10,000 - $99,999	10^4
5	$100,000 - $999,999	10^5
6	$1,000,000+	10^6

Likelihood

Based on the environment and current threat landscape, rated from 1 to 5, with 1 being unlkiley, and 5 being very likely

Control Maturity

Rated from 1 to 5, with 1 indicating the control has been implemented in a very limited or no capacity and 5 indicating the control is fully implemented. The maturity score represents mitigation of known threats to the University. Control implementation and likelihood of exploitation are inversely realted. A low maturity score indicates a higher likelihood that a vulnerability will exploited based on the lack of controls.

The maturity score is not an absolute measure, meaning the level of security required at the NSA to score a 5 differs from what the State Department of Revenue requires to score a 5, or what the University requires to score a 5. In this assessment a score of 5 represents the control maturity that would be aimed for given unlimited time and financial resources.

Mission Criticality

Rated from 1 to 5, with 1 indicating the control has little or no impact on the University mission and 5 indicating the control has a profound impact on the University mission.

Risk Score

The risk score is calculated by dividing the criticality rating by the status rating. This produces a value from 1 to 5 representing the assessment of risk to the University associated with a particular control set. 1 indicates the lowest risk possible and 5 indicates the highest risk possible.

Threats

ID	Description	Category (C.I.A)	Financial Impact
1	Ransomware	A	4
2	Disclosure of Information	C	5
3	Bank Fraud	C,A	6
4	Falsification of Records	I	5
5	Cyber attack on Physical Plant/Facilities	I	5
6	Denial of Service to Information Systems	A	4
7	Destruction of Records	I	4
8	Disclosure of Credentials	C	5
9	Social Engineering	C,I,A	6
10	Espionage	C	3
11	Loss of Electricity	A	5
12	Earthquake	A	6
13	Equipment Malfunction	I,A	4
14	Misuse of Information Systems Tools	C,I,A	5
15	Misuse of Audit Tools	C	5
16	Labor Disruption (Strike)	A	5
17	Terrorist Attack	C,I,A	6
18	Loss of Internet Connectivity	A	4
19	User Error	C,I,A	5
20	Lack/Loss of Vendor Support	A	5
21	Access by Proxy	C,I,A	6

Assessment 2019

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
CIS Control 1: Inventory and Control of Hardware Assets								
1.1	Utilize an Active Discovery Tool	Presence of and access from unauthorized devices on the network	1,2,5,6,10,21	27	5	135	2	81
1.2	Use a Passive Asset Discovery Tool							
1.3	Use DHCP Logging to Update Asset Inventory							
1.4	Maintain Detailed Asset Inventory							
1.5	Maintain Asset Inventory Information							
1.6	Address Unauthorized Assets							
1.7	Deploy Port Level Access Control							
1.8	Utilize Client Certificates to Authenticate Hardware Assets							
CIS Control 2: Inventory and Control of Software Assets								
2.1	Maintain Inventory of Authorized Software	Potential for use and execution of unauthorized and/or malicious software on institutional systems.	1,2,5,6,7,8,10,13,21	40	5	200	2	120
2.2	Ensure Software is Supported by Vendor							
2.3	Utilize Software Inventory Tools							
2.4	Track Software Inventory Information							
2.5	Intergrate Software and Hardware Asset Inventories							
2.6	Address Unapproved Software							
2.7	Utilize Application whitelisting							
2.8	Implement Application Whitelisting of Libraries							
2.9	Implement Application Whitelisting of scripts							
2.10	Physically or Logically Segregate High Risk Applications							
CIS Control 3: Continuous Vulnerability Management								
3.1	Run Automated Vulnerability Scanning Tools	Potential for exploitation of unpatched vulnerabilities on institutional systems.	1,2,5,6,7,8,10,21	36	5	180	2	108
3.2	Perfom Authenticated Vulnerability Scanning							
3.3	Protect Dedicated Assessment Accounts							
3.4	Deploy Automated Operating System Patch Management Tools							
3.5	Deploy Automated Software Patch Management Tools							
3.6	Compare Back-to-back Vulnerability Scans							
3.7	Utilize a Risk-rating Process							
CIS Control 4: Controlled Use of Administrative Privileges								
4.1	Maintain Inventory of Administrative Accounts	Potential for unauthorized or unintended use of administrative privileges on institutional systems.	1,2,4,5,7,8,10,14,15,19,21	52	5	260	3	104
4.2	Change Default Passwords							
4.3	Ensure the Use of Dedicated Administrative Accounts							
4.4	Use Unique Passwords							
4.5	Use Multifactor Authentication For All Administrative Access							
4.6	Use Dedicated Workstations For All Administratice Tasks							
4.7	Limit Access to Scripting Tools							
4.8	Log and Alert on Changes to Administrative Group Membership							
4.9	Log and Alert on Unsuccessful Administrative Account Login							

Assessment 2019

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers								
5.1	Establish Secure Configurations	Insecure system configurations stemming from operational inconsistency.	1,2,4,5,6,7,8, 10,14,15,21	51	5	255	4	51
5.2	Maintain Secure Images							
5.3	Securely Store Master Images							
5.4	Deploy System Configuration Managment Tools							
5.5	Implement Automated Configuration Monitoring Systems							
CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs								
6.1	Utilize Three Synchronized Time Sources	Inability to detect threats in a timely manner, and/or perform adequate incident analysis and response.	1,2,5,6,7,8,10,11,13,18,21	49	5	245	2	147
6.2	Activate Audit Logging							
6.3	Enable Detailed Logging							
6.4	Ensure Adequate Storage for Logs							
6.5	Central Log Management							
6.6	Deploy SIEM or Log Analytic Tools							
6.7	Regularly Review Logs							
6.8	Regularly Tune SIEM							
CIS Control 7: Email and Web Browser Protections								
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	End-user devices open to web and email based attacks.	1,2,3,4,5,7,8, 10,17,21	49	5	245	4	49
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins							
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients							
7.4	Maintain and Enforce Network-Based URL Filters							
7.5	Subscribe to URL-Categorization Service							
7.6	Log all URL Requests							
7.7	Use of DNS Filtering Services							
7.8	Implement DMARC and Enable Receiver-Side Verification							
7.9	Block Unnecessary File Types							
7.10	Sandbox All Email Attachments							
CIS Control 8: Malware Defenses								
8.1	Utilize Centrally Managed Anti-Malware Software	Inability to prevent and detect known threats.	1,2,3,4,5,6,7, 8,10,17,21	53	5	265	3	106
8.2	Ensure Anti-Malware Software and Signatures are Updated							
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies							
8.4	Configure Anti-Malware Scanning of Removable Devices							
8.5	Configure Devices to Not Auto-Run Content							
8.6	Centralize Anti-Malware Logging							
8.7	Enable DNS Query Logging							
8.8	Enable Command-Line Audit Logging							

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services								
9.1	Associate Active Ports, Services and Protocols to Asset Inventory	Presence of and access from unauthorized and potentially insecure devices on the network	1,2,3,4,5,6,7,8,10,17,21	53	5	265	3	106
9.2	Ensure Only Approved Ports, Protocols and Services Are Running							
9.3	Perform Regular Automated Port Scans							
9.4	Apply Host-Based Firewalls or Port Filtering							
9.5	Implement Application Firewalls							
CIS Control 10: Data Recovery Capabilities								
10.1	Ensure Regular Automated Backups	Inability to recover from data loss.	1,4,7,11,12,13,14,17,19	43	5	215	2	129
10.2	Perform Complete System Backups							
10.3	Test Data on Backup Media							
10.4	Protect Backups							
10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination							
CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches								
11.1	Maintain Standard Security Configurations for Network Devices	Insecurely configured network devices and potential for unauthorized access to critical network infrastructure.	2,5,6,8,10,15,17,18,21	43	5	215	3	86
11.2	Document Traffic Configuration Rules							
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes							
11.4	Install the Latest Stable Version of Any Security- Related Updates on All Network Devices							
11.5	Manage Network Devices Using Multi- Factor Authentication and Encrypted Sessions							
11.6	Use Dedicated Workstations For All Network Administrative Tasks							
11.7	Manage Network Infrastructure Through a Dedicated Network							
CIS Control 12: Boundary Defense								
12.1	Maintain an Inventory of Network Boundaries	Potential for unauthorized network traffic including malicious inbound traffic, unauthorized remote access and malicious traffic originating from the institutional network.	1,2,4,5,6,7,8,10,17,21	50	5	250	3	100
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries							
12.3	Deny Communications with Known Malicious IP Addresses							
12.4	Deny Communication over Unauthorized Ports							
12.5	Configure Monitoring Systems to Record Network Packets							
12.6	Deploy Network-Based IDS Sensors							
12.7	Deploy Network-Based Intrusion Prevention Systems							
12.8	Deploy NetFlow Collection on Networking Boundary Devices							
12.9	Deploy Application Layer Filtering Proxy Server							
12.10	Decrypt Network Traffic at Proxy							
12.11	Require All Remote Logins to Use Multi- Factor Authentication							
12.12	Manage All Devices Remotely Logging into Internal Network							
CIS Control 13: Data Protection								
13.1	Maintain an Inventory of Sensitive Information	Potential for unauthorized or unintentional access						

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	or unintentional access to, loss, or dissemination of sensitive data.	1,2,4,7,9,10	27	5	135	2	81
13.3	Monitor and Block Unauthorized Network Traffic							
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers							
13.5	Monitor and Detect Any Unauthorized Use of Encryption							
13.6	Encrypt the Hard Drive of All Mobile Devices							
13.7	Manage USB Devices							
13.8	Manage System's External Removable Media's Read/Write Configurations							
13.9	Encrypt Data on USB Storage Devices							
CIS Control 14: Controlled Access Based on the Need to Know								
14.1	Segment the Network Based on Sensitivity	Potential for unauthorized access to sensitive data.	1,2,5,6,8,10, 13,21	36	5	180	4	36
14.2	Enable Firewall Filtering Between VLANs							
14.3	Disable Workstation to Workstation Communication							
14.4	Encrypt All Sensitive Information in Transit							
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data							
14.6	Protect Information through Access Control Lists							
14.7	Enforce Access Control to Data through Automated Tools							
14.8	Encrypt Sensitive Information at Rest							
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data							
CIS Control 15: Wireless Access Control								
15.1	Maintain an Inventory of Authorized Wireless Access Points	Presence of and access from unauthorized and potentially insecure devices on the network	1,2,5,6,8,10, 21	32	5	160	2	96
15.2	Detect Wireless Access Points Connected to the Wired Network							
15.3	Use a Wireless Intrusion Detection System							
15.4	Disable Wireless Access on Devices if it is Not Required							
15.5	Limit Wireless Access on Client Devices							
15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients							
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data							
15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication							
15.9	Disable Wireless Peripheral Access to Devices							
15.10	Create Separate Wireless Network for Personal and Untrusted Devices							
CIS Control 16: Account Monitoring and Control								
16.1	Maintain an Inventory of Authentication Systems	Potential for unauthorized access to network resources.						
16.2	Configure Centralized Point of Authentication							
16.3	Require Multi-Factor Authentication							
16.4	Encrypt or Hash all Authentication Credentials							
16.5	Encrypt Transmittal of Username and Authentication Credentials							

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
16.6	Maintain an Inventory of Accounts		1,2,5,6,8,10, 13,21	36	5	180	4	36
16.7	Establish Process for Revoking Access							
16.8	Disable Any Unassociated Accounts							
16.9	Disable Dormant Accounts							
16.10	Ensure All Accounts Have An Expiration Date							
16.11	Lock Workstation Sessions After Inactivity							
16.12	Monitor Attempts to Access Deactivated Accounts							
16.13	Alert on Account Login Behavior Deviation							
CIS Control 17: Implement a Security Awarness and Training Proogram								
17.1	Perform a Skills Gap Analysis	Potential for accidental breach of data security by employees.	1,2,3,7,8,9,1 0,14,15,19	48	5	240	2	144
17.2	Deliver Training to Fill the Skills Gap							
17.3	Implement a Security Awareness Program							
17.4	Update Awareness Content Frequently							
17.5	Train Workforce on Secure Authentication							
17.6	Train Workforce on Identifying Social Engineering Attacks							
17.7	Train Workforce on Sensitive Data Handling							
17.8	Train Workforce on Causes of Unintentional Data Exposure							
17.9	Train Workforce Members on Identifying and Reporting Incidents							
CIS Control 18: Appplication Software Security								
18.1	Establish Secure Coding Practices	Potential for use and execution of insecure code/software on institutional systems and/or with sensitive data.	1,2,4,5,6,7,8, 10,19,21	46	5	230	2	138
18.2	Ensure Explicit Error Checking is Performed for All In-House Developed Software							
18.3	Verify That Acquired Software is Still Supported							
18.4	Only Use Up-to-Date And Trusted Third-Party Components							
18.5	Only Standardized and Extensively Reviewed Encryption Algorithms							
18.6	Ensure Software Development Personnel are Trained in Secure Coding							
18.7	Apply Static and Dynamic Code Analysis Tools							
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities							
18.9	Separate Production and Non-Production Systems							
18.10	Deploy Web Application Firewalls							
18.11	Use Standard Hardening Configuration Templates for Databases							
CIS Control 19: Incident Response and Management								
19.1	Document Incident Response Procedures	Inability to respond to incidents in a timely and effective manner.	1,2,3,4,5,6,7, 8,9,10,11,12, 13,14,15,16,	103	5	515	4	103
19.2	Assign Job Titles and Duties for Incident Response							
19.3	Designate Management Personnel to Support Incident Handling							
19.4	Devise Organization-wide Standards for Reporting Incidents							
19.5	Maintain Contact Information For Reporting Security Incidents							

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
19.6	Publish Information Regarding Reporting Computer Anomalies andIncidents		17,18,19,20,21					
19.7	Conduct Periodic Incident Scenario Sessions for Personnel							
19.8	Create Incident Scoring and Prioritization Schema							
CIS Control 20: Penetration Tests and Red Team Exercises								
20.1	Establish a Penetration Testing Program	Unmitigated vulnerabilities that may be exploited by malicious actors due to ineffective detection and planning.	1,2,5,6,7,8,10,21	36	5	180	1	144
20.2	Conduct Regular External and Internal Penetration Tests							
20.3	Perform Periodic Red Team Exercises							
20.4	Include Tests for Presence of Unprotected System Information and Artifacts							
20.5	Create a Test Bed for Elements Not Typically Tested in Production							
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert							
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards							
20.8	Control and Monitor Accounts Associated with Penetration Testing							

Assessment 2020

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
CIS Control 1: Inventory and Control of Hardware Assets								
1.1	Utilize an Active Discovery Tool	Presence of and access from unauthorized devices on the network	1,2,5,6,10, 21	27	4	108	2.5	54
1.2	Use a Passive Asset Discovery Tool							
1.3	Use DHCP Logging to Update Asset Inventory							
1.4	Maintain Detailed Asset Inventory							
1.5	Maintain Asset Inventory Information							
1.6	Address Unauthorized Assets							
1.7	Deploy Port Level Access Control							
1.8	Utilize Client Certificates to Authenticate Hardware Assets							
CIS Control 2: Inventory and Control of Software Assets								
2.1	Maintain Inventory of Authorized Software	Potential for use and execution of unauthorized and/or malicious software on institutional systems.	1,2,5,6,7,8, 10,13,21	40	5	200	1.5	140
2.2	Ensure Software is Supported by Vendor							
2.3	Utilize Software Inventory Tools							
2.4	Track Software Inventory Information							
2.5	Integrate Software and Hardware Asset Inventories							
2.6	Address Unapproved Software							
2.7	Utilize Application Safelisting							
2.8	Implement Application Safelisting of Libraries							
2.9	Implement Application Safelisting of scripts							
2.10	Physically or Logically Segregate High Risk Applications							
CIS Control 3: Continuous Vulnerability Management								
3.1	Run Automated Vulnerability Scanning Tools	Potential for exploitation of unpatched vulnerabilities on institutional systems.	1,2,5,6,7,8, 10,21	36	5	180	2	108
3.2	Perfom Authenticated Vulnerability Scanning							
3.3	Protect Dedicated Assessment Accounts							
3.4	Deploy Automated Operating System Patch Management Tools							
3.5	Deploy Automated Software Patch Management Tools							
3.6	Compare Back-to-back Vulnerability Scans							
3.7	Utilize a Risk-rating Process							
CIS Control 4: Controlled Use of Administrative Privileges								
4.1	Maintain Inventory of Administrative Accounts	Potential for unauthorized or unintended use of administrative privileges on institutional systems.	1,2,4,5,7,8, 10,14,15,1 9,21	52	5	260	3.5	78
4.2	Change Default Passwords							
4.3	Ensure the Use of Dedicated Administrative Accounts							
4.4	Use Unique Passwords							
4.5	Use Multifactor Authentication For All Administrative Access							
4.6	Use Dedicated Workstations For All Administratice Tasks							
4.7	Limit Access to Scripting Tools							
4.8	Log and Alert on Changes to Administrative Group Membership							
4.9	Log and Alert on Unsuccessful Administrative Account Login							

Assessment 2020

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers								
5.1	Establish Secure Configurations	Insecure system configurations stemming from operational inconsistency.	1,2,4,5,6,7,8,10,14,15,21	51	5	255	4	51
5.2	Maintain Secure Images							
5.3	Securely Store Master Images							
5.4	Deploy System Configuration Management Tools							
5.5	Implement Automated Configuration Monitoring Systems							
CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs								
6.1	Utilize Three Synchronized Time Sources	Inability to detect threats in a timely manner, and/or perform adequate incident analysis and response.	1,2,5,6,7,8,10,11,13,18,21	49	5	245	2	147
6.2	Activate Audit Logging							
6.3	Enable Detailed Logging							
6.4	Ensure Adequate Storage for Logs							
6.5	Central Log Management							
6.6	Deploy SIEM or Log Analytic Tools							
6.7	Regularly Review Logs							
6.8	Regularly Tune SIEM							
CIS Control 7: Email and Web Browser Protections								
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	End-user devices open to web and email based attacks.	1,2,3,4,5,7,8,10,17,21	49	5	245	4	49
7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins							
7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients							
7.4	Maintain and Enforce Network-Based URL Filters							
7.5	Subscribe to URL-Categorization Service							
7.6	Log all URL Requests							
7.7	Use of DNS Filtering Services							
7.8	Implement DMARC and Enable Receiver-Side Verification							
7.9	Block Unnecessary File Types							
7.10	Sandbox All Email Attachments							
CIS Control 8: Malware Defenses								
8.1	Utilize Centrally Managed Anti-Malware Software	Inability to prevent and detect known threats.	1,2,3,4,5,6,7,8,10,17,21	53	5	265	3	106
8.2	Ensure Anti-Malware Software and Signatures are Updated							
8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies							
8.4	Configure Anti-Malware Scanning of Removable Devices							
8.5	Configure Devices to Not Auto-Run Content							
8.6	Centralize Anti-Malware Logging							
8.7	Enable DNS Query Logging							
8.8	Enable Command-Line Audit Logging							

Assessment 2020

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services								
9.1	Associate Active Ports, Services and Protocols to Asset Inventory	Presence of and access from unauthorized and potentially insecure devices on the network	1,2,3,4,5,6,7,8,10,17,21	53	4	212	3	84.8
9.2	Ensure Only Approved Ports, Protocols and Services Are Running							
9.3	Perform Regular Automated Port Scans							
9.4	Apply Host-Based Firewalls or Port Filtering							
9.5	Implement Application Firewalls							
CIS Control 10: Data Recovery Capabilities								
10.1	Ensure Regular Automated Backups	Inability to recover from data loss.	1,4,7,11,12,13,14,17,19	43	5	215	2	129
10.2	Perform Complete System Backups							
10.3	Test Data on Backup Media							
10.4	Protect Backups							
10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination							
CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches								
11.1	Maintain Standard Security Configurations for Network Devices	Insecurely configured network devices and potential for unauthorized access to critical network infrastructure.	2,5,6,8,10,15,17,18,21	43	5	215	3	86
11.2	Document Traffic Configuration Rules							
11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes							
11.4	Install the Latest Stable Version of Any Security- Related Updates on All Network Devices							
11.5	Manage Network Devices Using Multi- Factor Authentication and Encrypted Sessions							
11.6	Use Dedicated Workstations For All Network Administrative Tasks							
11.7	Manage Network Infrastructure Through a Dedicated Network							
CIS Control 12: Boundary Defense								
12.1	Maintain an Inventory of Network Boundaries	Potential for unauthorized network traffic including malicious inbound traffic, unauthorized remote access and malicious traffic originating from the institutional network.	1,2,4,5,6,7,8,10,17,21	50	5	250	3.5	75
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries							
12.3	Deny Communications with Known Malicious IP Addresses							
12.4	Deny Communication over Unauthorized Ports							
12.5	Configure Monitoring Systems to Record Network Packets							
12.6	Deploy Network-Based IDS Sensors							
12.7	Deploy Network-Based Intrusion Prevention Systems							
12.8	Deploy NetFlow Collection on Networking Boundary Devices							
12.9	Deploy Application Layer Filtering Proxy Server							
12.10	Decrypt Network Traffic at Proxy							
12.11	Require All Remote Logins to Use Multi- Factor Authentication							
12.12	Manage All Devices Remotely Logging into Internal Network							
CIS Control 13: Data Protection								
13.1	Maintain an Inventory of Sensitive Information	Potential for unauthorized or unintentional access						

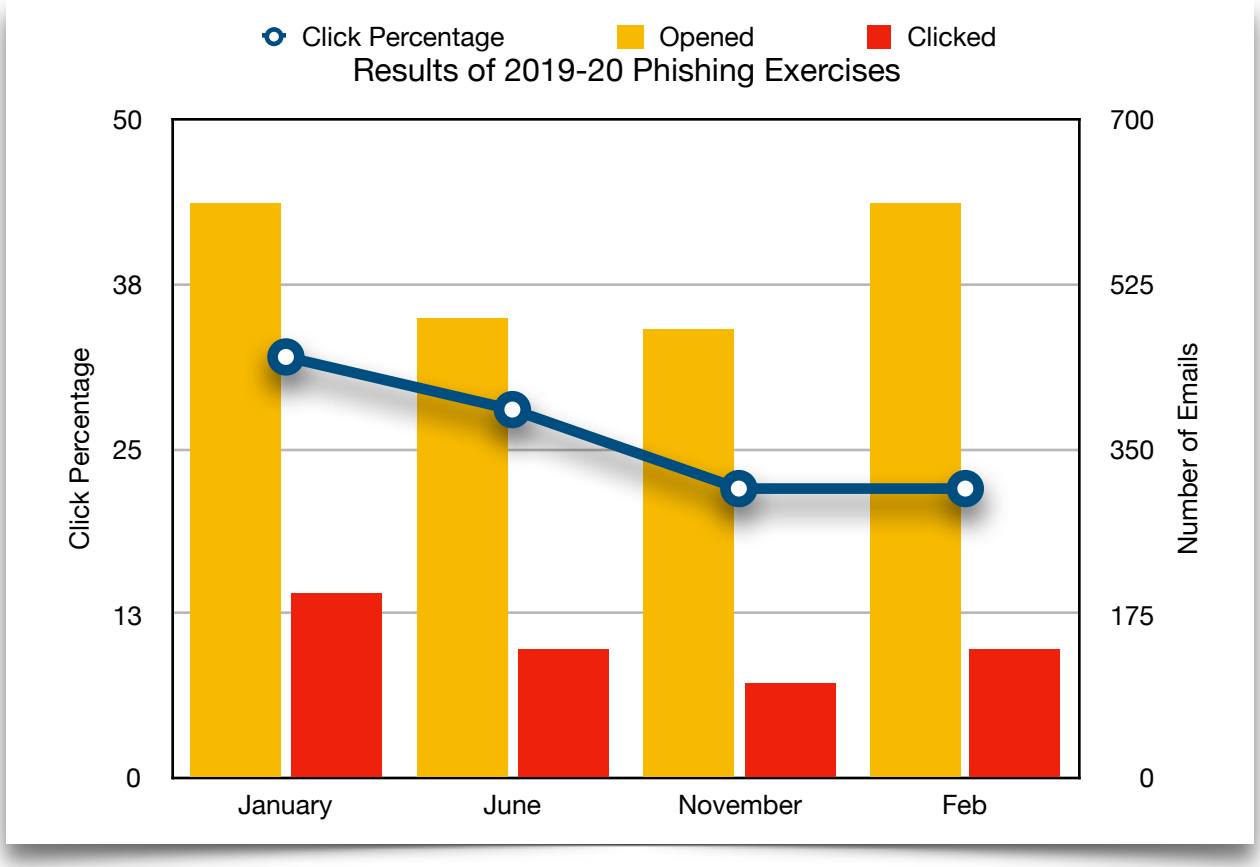
Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	or unintentional access to, loss, or dissemination of sensitive data.	1,2,4,7,9,10	27	5	135	1.5	94.5
13.3	Monitor and Block Unauthorized Network Traffic							
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers							
13.5	Monitor and Detect Any Unauthorized Use of Encryption							
13.6	Encrypt the Hard Drive of All Mobile Devices							
13.7	Manage USB Devices							
13.8	Manage System's External Removable Media's Read/Write Configurations							
13.9	Encrypt Data on USB Storage Devices							
CIS Control 14: Controlled Access Based on the Need to Know								
14.1	Segment the Network Based on Sensitivity	Potential for unauthorized access to sensitive data.	1,2,5,6,8,10,13,21	36	5	180	4	36
14.2	Enable Firewall Filtering Between VLANs							
14.3	Disable Workstation to Workstation Communication							
14.4	Encrypt All Sensitive Information in Transit							
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data							
14.6	Protect Information through Access Control Lists							
14.7	Enforce Access Control to Data through Automated Tools							
14.8	Encrypt Sensitive Information at Rest							
14.9	Enforce Detail Logging for Access or Changes to Sensitive Data							
CIS Control 15: Wireless Access Control								
15.1	Maintain an Inventory of Authorized Wireless Access Points	Presence of and access from unauthorized and potentially insecure devices on the network	1,2,5,6,8,10,21	32	4	128	2	76.8
15.2	Detect Wireless Access Points Connected to the Wired Network							
15.3	Use a Wireless Intrusion Detection System							
15.4	Disable Wireless Access on Devices if it is Not Required							
15.5	Limit Wireless Access on Client Devices							
15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients							
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data							
15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication							
15.9	Disable Wireless Peripheral Access to Devices							
15.10	Create Separate Wireless Network for Personal and Untrusted Devices							
CIS Control 16: Account Monitoring and Control								
16.1	Maintain an Inventory of Authentication Systems	Potential for unauthorized access to network resources.						
16.2	Configure Centralized Point of Authentication							
16.3	Require Multi-Factor Authentication							
16.4	Encrypt or Hash all Authentication Credentials							
16.5	Encrypt Transmittal of Username and Authentication Credentials							

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
16.6	Maintain an Inventory of Accounts		1,2,5,6,8,10,13,21	36	5	180	4	36
16.7	Establish Process for Revoking Access							
16.8	Disable Any Unassociated Accounts							
16.9	Disable Dormant Accounts							
16.10	Ensure All Accounts Have An Expiration Date							
16.11	Lock Workstation Sessions After Inactivity							
16.12	Monitor Attempts to Access Deactivated Accounts							
16.13	Alert on Account Login Behavior Deviation							
CIS Control 17: Implement a Security Awarness and Training Proogram								
17.1	Perform a Skills Gap Analysis	Potential for accidental breach of data security by employees.	1,2,3,7,8,9,10,14,15,19	48	5	240	3.5	72
17.2	Deliver Training to Fill the Skills Gap							
17.3	Implement a Security Awareness Program							
17.4	Update Awareness Content Frequently							
17.5	Train Workforce on Secure Authentication							
17.6	Train Workforce on Identifying Social Engineering Attacks							
17.7	Train Workforce on Sensitive Data Handling							
17.8	Train Workforce on Causes of Unintentional Data Exposure							
17.9	Train Workforce Members on Identifying and Reporting Incidents							
CIS Control 18: Appplication Software Security								
18.1	Establish Secure Coding Practices	Potential for use and execution of insecure code/software on institutional systems and/or with sensitive data.	1,2,4,5,6,7,8,10,19,21	46	5	230	3	92
18.2	Ensure Explicit Error Checking is Performed for All In-House Developed Software							
18.3	Verify That Acquired Software is Still Supported							
18.4	Only Use Up-to-Date And Trusted Third-Party Components							
18.5	Only Standardized and Extensively Reviewed Encryption Algorithms							
18.6	Ensure Software Development Personnel are Trained in Secure Coding							
18.7	Apply Static and Dynamic Code Analysis Tools							
18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities							
18.9	Separate Production and Non-Production Systems							
18.10	Deploy Web Application Firewalls							
18.11	Use Standard Hardening Configuration Templates for Databases							
CIS Control 19: Incident Response and Management								
19.1	Document Incident Response Procedures	Inability to respond to incidents in a timely and effective manner.	1,2,3,4,5,6,7,8,9,10,11,12,13,14,1	103	5	515	3	206
19.2	Assign Job Titles and Duties for Incident Response							
19.3	Designate Management Personnel to Support Incident Handling							
19.4	Devise Organization-wide Standards for Reporting Incidents							
19.5	Maintain Contact Information For Reporting Security Incidents							

Control ID	Control Description	Vulnerability Addressed	Threat(s) Mitigated	Financial Impact	Likelihood	Risk Score	Control Maturity	Unmitigated Risk
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents		5,16,17,18, 19,20,21					
19.7	Conduct Periodic Incident Scenario Sessions for Personnel							
19.8	Create Incident Scoring and Prioritization Schema							
CIS Control 20: Penetration Tests and Red Team Exercises								
20.1	Establish a Penetration Testing Program	Unmitigated vulnerabilities that may be exploited by malicious actors due to ineffective detection and planning.	1,2,5,6,7,8, 10,21	36	5	180	1	144
20.2	Conduct Regular External and Internal Penetration Tests							
20.3	Perform Periodic Red Team Exercises							
20.4	Include Tests for Presence of Unprotected System Information and Artifacts							
20.5	Create a Test Bed for Elements Not Typically Tested in Production							
20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert							
20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards							
20.8	Control and Monitor Accounts Associated with Penetration Testing							

Cybersecurity Hot-sheet Feb. 2020

Feb. 2020 Employee-related Risk: Med. High



	January	June	November	Feb - 2020
Type	Unannounced	Announced	Announced	Unannounced
Difficulty	Challenging	Easy	Easy	Medium
Click Rate	32% of opened emails	28% of opened emails	22% of opened emails	22% of opened emails
Risk	High	Equal or higher	Reduced, still too high	Steady, improved by 31%

Summary

- At the end of January, I.T. ran the infamous initial phishing exercise to establish a baseline for phishing susceptibility.
- At the end of June, I.T. ran another phishing exercise where the exercise was announced in an all-campus email sent by the CIO.
  - The June exercise also only used spoofs of external entities that were non-threatening in nature. No spoofs of internal SOU email addresses were used.
- In November, I.T. ran a phishing exercise that was announced, using non-threatening and low to medium difficulty emails
- In February of 2020, I.T. ran an unannounced campaign to compare to 2019's baseline.
  - This campaign ranked low to medium for difficulty.

The target click-percentage that we are hoping to reach is 4% to 5% (2018, Verizon 2018 Breach Investigations Report). **SOU is now hovering around 22%**.

The data shows that our phishing exercises are having an impact. The click-rate has decreased 5% to 10%-points or by 31% overall.

Recommendations

- SOU should immediately begin the proposed mandatory cybersecurity training campaign, starting this summer with employees and expanding to include faculty when they return in September.
  - The training should be required immediately for those who have been clicking in the phishing emails.
- SOU's email policy should be updated to strongly suggest that SOU employees use personal email accounts for personal business. This may reduce the likelihood that employees click in spoofed marketing emails sent to their SOU accounts.
- I.T. should continue the phishing campaigns **on a more frequent basis**.
- I.T. should continue to provide multiple modes of training (classroom and video).

Governance Work Group Update

Future Meetings

Adjournment