October 1, 2019

Board of Trustees
Initial Quarterly Report

Per your request, I have compiled a report that covers three separate areas of Risk Management at Winthrop:

1. IT Compliance activities (aka Information Security)

This is a new area split from IT operations in June 2019. The President has approved an implementation plan for Information Security and I have attached a detailed summary of activities during these first four months relating to compliance under this plan.

I will note there is a finding in our annual external audit report relating to compliance under the Graham Leach Bliley Act which covers the protection of financial data. The recommendation from the external auditor is for Winthrop to complete our implementation plan. As a requirement under this act, we are asking the Board to adopt a resolution authorizing the administration to implement a comprehensive information security plan at Winthrop University.

2. Pending litigation/legal issues-confidential

There is a spreadsheet attached with current legal issues facing the University. Party names and other sensitive data have been removed. However, be aware that some items listed are only potential claims and not subject to release to the public.

I was asked to list the maximum potential loss to the University for each pending matter. However, that is not usually known in matters outside of those covered by insurance. Many lawsuits now ask for any damages the court is willing to award, so there is not always a set risk known until we reach the mediation stage. Where that potential liability is known, I have noted it on the spreadsheet.

3. Workers Compensation claims-confidential

The State Accident Fund (SAF) is the agency that handles all of Winthrop University's workers compensation claims. I have attached a spreadsheet of open claims with the State Accident Fund. There are also two years of claim history in order to provide a baseline of activity.

I am happy to answer any questions or discuss any of these items in detail.

Sincerely,

Caroline Overcash

Caroline Craig Overcash, Esq., CPM, CISA | Director of Internal Audit and Compliance | Winthrop University
Internal Audit | 108 Tillman | Rock Hill, SC 29733
Tel: 803.323.4698 | overcashc@winthrop.edu
Veritas cum libertate

October 1, 2019

Board of Trustees
Initial Quarterly Report

IT Compliance activities (aka Information Security)

Background:

On June 1st 2019, Information Security was moved under Internal Audit and Compliance at Winthrop. Prior to that time, everything was housed in Computing and Information Technology (IT). The change was made in accordance with best practices to have information security report up separately from IT to Senior Leadership at the University.

Privacy (information classification) also reports through Internal Audit and functions through an Enterprise-wide committee with representation from all parts of campus. This committee has several sub-committees charged with particular data protection standards relevant to Winthrop University, e.g. FERPA, HIPAA, GLBA, PCI-DSS, CJIS.

At this time, Privacy and Information Security report to Internal Audit which has a direct report to the President and the Board. IT now reports to the VP for Business and Finance which also directly reports to the President. This separation of reporting structure from IT is recommended by the SC State Division of Administration as a best practice.

Summary of Sections of the Winthrop Information Security Implementation Plan currently active

Part 1: Privacy/data

Members of the privacy committee have been charged with the following tasks during this quarter:

1. **Creation of privacy statements relative to each functional area of the University.**
    a. All of members work within their sub-committees.
    b. Draft statements are reviewed with legal for compliance prior to publication
    c. All statements provide a link to the University Privacy Policy.
    d. Statements are published on all applicable webpages
    e. Statements are reviewed by committee members annually.

Status: In progress

Target date for drafts:	June 1, 2019
Target date for finalized statements:	October 31, 2019
Target date for all statements published and correctly linked:	December 15, 2019

27 number of members have submitted drafts and are re-working revisions from legal.
4 number have not yet turned in statements (late adds-behind project schedule)

2. **Completion of a data inventory and classification by each functional area of the University.**
    a. All areas work to document business processes
    b. All processes shows data elements used.

c. All data used are classified under the state schema (public, internal, confidential, and restricted).

Status: In progress
Target date for drafts: December 15, 2019
20 number of members have submitted inventory and classification schemes.
12 number of members still need to meet for extended training sessions.

Part 2 Information Security

Began June 2019

1. **Funding:**
    a. Awaiting budget approval from Business and Finance to fund operations for information security presented April 2019 in anticipation of move into Internal Audit.

Status: Delayed
Budget submitted April 2019
Target date for budget approval: June 2019

b. Requested limited state determined Priority 0 (extreme) and Priority 1 (top) needs to address critical operational gaps.

Status: Delayed
Budget Approval Date June 2019
RFP development and submission (procurement) July 2019
Vendor approval and contract finalization September 2019
Solution deployment October 2019

2. **Governance**
    a. BoT Resolution authorizing development of WU security plan

Status: In development
Target date: October 2019 BoT meeting

b. Policy Development
    i. Infosec drafts policies that align with the 13 policy areas mandated by the state in SC-DIS 200.
    ii. Infosec reviews DIS-200 along with NIST revisions to determine gaps
    iii. Infosec Winthrop drafts additional policies to ensure compliance with federal data security standards.
    iv. Policies review by legal
    v. Finalized Policies submitted to Winthrop Senior Leadership for approval and adoption.
    vi. Adopted policies promulgated to Winthrop population

Status: In development
Target date for drafts: October 2019

12 policy drafts out of 13 are complete

Target date for review: **November 2019**
Target date for adoption/promulgation: **Beginning November 2019**

c. Related procedure development
    i. IT practices formalized into written procedures and guides that are in compliance with University policy.
    ii. Gaps addressed and new procedures developed to implement all parts of University Infosec policy.

Status: Not yet started
Target date for drafts: **November 2019**
Target date for review: **January 2020**
Target date for finalized procedures: **March 2020**

3. Risk Assessment/Gap Analysis:

a. Risk assessment covers 400 controls in the InfoSec matrix as created by the SC State Department of Administration Division of Information Security.
b. Risk assessment requires working with key stakeholders across divisions to correctly baseline security standards at Winthrop.

Status: In Progress
Target date for finalizing: **October 31, 2019**

Once the Risk Assessment and Gap analysis are completed, I plan to have a heat map and dashboard for compliance available for Board review.

Sincerely,

Caroline Overcash

Caroline Craig Overcash, Esq., CPM, CISA | Director of Internal Audit and Compliance | Winthrop University
Internal Audit | 108 Tillman | Rock Hill, SC 29733
Tel: 803.323.4698 | overcashc@winthrop.edu
Veritas cum libertate