# IT Security, Including Risk Management Report

## BACKGROUND

In 2016, the Executive & Audit Committee approved a model for developing action plans to mitigate the top risks that may hinder OSU's ability to achieve the objectives outlined in Strategic Plan 3.0. Each of the identified top risks was assigned to the various Board committees based on alignment with each committee's charter and workload.

## STATUS UPDATE

Over the last two years, the Executive & Audit Committee has provided oversight of the university's risk action plan related to IT security, one of the top risks assigned to the committee. To address this risk, the university has created a security program, which includes formal risk assessments. These have been conducted and communicated annually since 2016. As the threat environment continually worsens, we are evaluating how to enhance the risk assessment process and the overall security program with a focus on mitigating the most pressing risk areas. These efforts are described in the annual progress report in Attachment 1.

## NEXT STEPS

At the April 2018 meeting, the committee will review the progress report with staff and may identify additional follow-up, as needed.

# Oregon State University
# University Risk Management
# 2016-17 Priorities
# Information Technology Security

| Board Oversight Committee | Risk Topic | University Goal | Type(s) of Risks to be Prevented | Risk Owner(s) | Primary Risk Mitigation Strategy(ies)[1] | Risk Mitigation Team |
|---|---|---|---|---|---|---|
| Executive & Audit Committee | Information Technology (IT) Security | Efficient IT systems that meet strategic needs and ensure continuity of service to the campus | Operational, Compliance, Financial, Reputational | Provost, Chief Information Officer (CIO) | Accept, Reduce, Share/Insure | Chief Information Security Officer,<br>Associate Provost of Infrastructure and Operations,<br>Director of Enterprise Computing,<br>IT Security Governance Council |

## Mitigation Plan

| Objectives to Achieve | Actions Underway | Status Report |
|---|---|---|
| 1. Identify and communicate risks | a. Perform annual assessment of systems and infrastructure<br>b. Enhance existing assessment framework to provide additional insight including benchmarking progress against other universities<br>c. Communicate results to Campus Executive Compliance Committee (CEC) and IT Security Council on cost/benefit analysis. | Initial risk assessment completed in January 2018. Additional assessment scheduled for spring/summer 2018. Review with IT Security Governance Council and CEC in fall 2018. |

[1] Definitions of mitigation strategies:
Avoid: Discontinue the activities that present unacceptable risk
Share/Insure: Transfer the risk through insurance programs or 3rd party
Reduce: Implement controls, practices, programs to lessen the risk
Accept: Proceed with the activity because the benefit outweighs the risk

| Mitigation Plan (continued) | | |
|---|---|---|
| **Objectives to Achieve** | **Actions Underway** | **Status Report** |
| 2. Develop and implement mitigation plans for risks identified in January 2018 assessment and in audits. | The following actions have been identified as having the potential to mitigate risk significantly, and will be scoped and prioritized appropriately:<br>• Improve ability to assess whether identified vulnerabilities were corrected.<br>• Evaluate processes for scanning employee systems for inappropriately stored Social Security Numbers (SSNs).<br>• Eliminate OSU-Access wireless network.<br>• Provide additional employee training for security.<br>• Consider moving Exchange email/calendar to the cloud<br>• Review network architecture for the need for potential additional firebreaks.<br>• Provide a mechanism for a complete inventory of devices connected to the network.<br>• Mitigate actions identified in audits. | Report reviewed by IT Security Governance Council in February 2018.<br><br>Complete assessment and plan by July 31, 2018. Plan will include any phasing necessary to align with available funding.<br><br>Status reports will be provided to IT Security Governance and CEC throughout 2018. |

## Performance Metrics

| Metric | Current Measure | Goal | Comments |
|---|---|---|---|
| As outlined in Objective #1, benchmarking will include an analysis of best practice metrics. Future reports will be adjusted accordingly. | To be determined | To be determined | |

## Plan Review and Report Schedule

| Action | Oversight Group | Completion Date or Frequency of Action | Comments |
|---|---|---|---|
| Review annual progress report, including trends and significant incidents; schedule educational and discussion items as requested by the Executive & Audit Committee. | IT Security Governance Council, CEC and appropriate leadership councils | Annually (progress report) | |

| **Plan Review and Report Schedule (continued)** | | | |
|---|---|---|---|
| **Action** | **Oversight Group** | **Completion Date or Frequency of Action** | **Comments** |
| IT Security Plan Update | Campus Compliance Executive Committee | Annually | |
| Review annual IT security plan | IT Security Governance Council, Provost, and Vice President of Finance and Administration | Annually | |