IT Audit Processes and 2016 Email Audit

2017

What is an IT Audit?

- an examination of the practices, procedures, and management controls within an information technology (IT) infrastructure.

Auditing Agencies

- Federal
  - Typically grant-related
  - Reports go to granting federal agency
- Louisiana Legislative
  - Reports go to Legislature
- LSU Internal
  - Reports go to University leadership

Process for Addressing IT Audits

1. Receive audit findings from Internal Audit.
2. Draft management response to audit findings.
3. CFO and Provost approve management response.
4. Communicate audit findings, responses, and initial timetable to departmental Technology Support Personnel (TSP) so they can absorb and respond.
5. Develop draft policy language through security advisory committee.
6. Submit draft policy to Academic Affairs for formal process and review by affected stakeholders.
7. Receive and merge concerns from TSP's and stakeholders.
8. Determine which concerns can be addressed relative to the findings and how. Develop strategy or strategies to address.
9. Surface identified issues and strategies with ITS Faculty IT Advisory Council and other groups with interest.
10. Revisit with internal audit and senior departmental admins to evolve strategies.
11. Iterate to step 7 until all issues resolved or decisions rendered.

2016 Email Audit

- Conducted by LSU Internal Audit in early 2016
- Areas of Focus
  - Proper retention of email
  - Disaster recovery and business continuity planning
  - Logical and physical security
- Initial findings presented in July of 2016
- Management response and final report in November 2016

2016 Email Audit Findings

- 5 Findings
- 3 Findings affect the Baton Rouge campus

Finding 1

- Finding
  - LSU management should revise PS 6.15, "Email Use Policy" to recognize the institution's responsibility for ensuring compliance with retention requirements.
- Response
  - *The LSU IT Security and Policy Group will convene an advisory group and begin the process of revising PS 06.15 and possibly other information security policies in the current fiscal year (FY17).*

Finding 2

- Finding
  - LSU should take steps to implement the legal hold or archival controls of emails as soon as possible. LSU ITS has tested and is prepared to deploy legal hold controls for the campus-wide Office 365 email system. The legal hold controls provided will ensure that emails are retained as required.
- Response
  - *Implemented August 1, 2016 (for central email systems).*

Finding 3

- Finding
  - **All departments currently operating independent email systems, with the exceptions noted below, should begin migration of users to the LSU Office365 email system.** All employees on the LSU campus are provided with an LSU email account within the Office 365 system deployed by LSU ITS. This recommended action would provide email services at no additional cost to departments and would eliminate unnecessary duplication of services. The migration of email to the LSU Office 365 email system will also provide the necessary controls to address the legal requirements for email retention following the implementation of Recommendation 2.
- Response
  - *The LSU IT Security and Policy Group will begin developing a tentative plan for migrating unit email services to the central Office 365 service in the current fiscal year.*
- Notes
  - Louisiana Revised Statutes, Title 44

Status of the Mitigation Process for the 2016 Email Audit

1. Receive audit findings from Internal Audit.
2. Draft management response to audit findings.
3. CFO and Provost approve management response.
4. Communicate audit findings, responses, and initial timetable to departmental Technology Support Personnel (TSP) so they can absorb and respond.
5. **Develop draft policy language through security advisory committee.**
6. Submit draft policy to Academic Affairs for formal process.
7. Receive and merge concerns from TSP's and senior departmental admins.
8. Determine which concerns can be addressed relative to the findings and how. Develop strategy or strategies to address.
9. Surface issues and strategies with ITS Faculty IT Advisory Council and other groups with interest.
10. Revisit with internal audit and senior departmental admins to evolve strategies.
11. Iterate to step 7 until all issues resolved.

Draft Policy Language

- **General Policy**
  - LSU owns all LSU.EDU e-mail addresses/ accounts/ boxes. E-mail addresses/ accounts/ boxes are assigned to individuals as a tool for facilitating teaching, research, and conducting University business.
  - Primary e-mail accounts are not to be transferred to any other person; however, primary e-mail accounts may be shared with another individual, based on business requirements.

Draft Policy Language

- **Naming Convention** (email accounts)
  - Employees and affiliated individuals who are granted an LSU e-mail account will receive an address in a format and design determined by the University that is distinguishable, as well as unique.
- **Departmental Email Services**
  - The University is required to comply with Louisiana R.S.Title 44 which outlines the requirements for retention or archiving of e-mail. Thus, University departments shall not operate their own departmental e-mail services in order to facilitate compliance and public records requests.

Draft Policy Language

- **Email Retraction**
  - The University's Information Security Team may also retract messages from University e-mail accounts that have been identified to be malicious and intended to cause harm to the University community, systems and/or network. Any retraction to be conducted by the Information Security Team shall be provided to the Chief Information Security Officer (CISO) in writing and approved prior to being implemented.

What's next?

- Formal review of policy language through Academic Affairs established process
- Documentation and validation of any business requirements surfaced by TSP's and reviewers
- University decision on the question of branding
- Selection and implementation of new Identity and Access Management System (IAM) and other IT solutions to address identified and accepted business requirements.

Questions?