Texas Higher Education
COORDINATING BOARD

Data Modernization Initiative Review & Advise

Interim Status Report March 2022

1

Review and Advisory Services

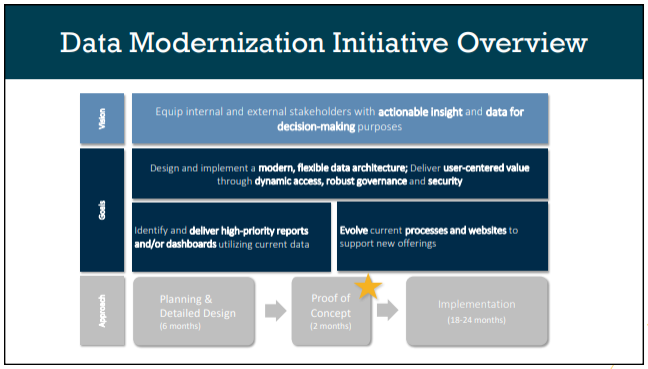
- Differences from a standard Internal Audit engagement:
- Programs are reviewed while they are being administered versus a lookback period
- Feedback is provided to management throughout the engagement
- Results are periodically summarized in interim status reports
- Reports look different
- Important guard rails are monitored throughout engagement – see slide 8.

THECB Texas Higher Education COORDINATING BOARD

2

2

DMI Overview: Vision, Goals, Approach



Advisory/Nonaudit Services: What we reviewed

As part of our advisory services, we initially reviewed the following related to security controls in the first phase of the DMI review. As we move forward, we will review other areas of the DMI project.

DMI Roadmaps, infrastructure documentation, contracts, responsible, accountable, consulted, informed (RACI) charts, Azure Security Center documents, applicable security controls such as National Institute of Standards and Technology (NIST), and interviewed various staff members.

Summary Observations

- Security control implementation is underway and encompasses what we expect to see at this stage.
- Staff are implementing security controls with available resources. Resources may need to be adjusted as the cloud portfolio grows.
- Documentation of security controls is ongoing and updated as needed.
- THECB is using contractors to fill skills gaps, however moving forward internal staff and new staff will need to possess skills previously filled by contractors.
- The DMI project followed the appropriate process for procuring cloud resources.
- Some legacy systems outside the scope of the DMI were brought to our attention during this review that may not have followed a process that appropriately involved ISS before the system(s) was procured. ISS is (1) working with the procurement team to ensure that appropriate coordination of effort exists, and (2) that future risk assessment exercises will train users on requirements.

Internal Audit Recommendations

Risks:

Inventory of Cloud Resources:

1. Without a streamlined inventory process of cloud resources THECB could be unable to verify systems and identify responsibilities for each system. Staff may be unclear as to their roles and responsibilities related to the support of cloud systems.

Risk Assessments:

2. Failure to add the DMI to established annual risk assessment processes may results in gaps in the evaluation of future cloud initiatives, security deficiencies, etc.

Resource Planning/Hiring:

3. Without specialized security staff the agency is at risk for improper incident detection, delays in project completion, lack of review over critical projects, and compliance with TAC202.

Recommendations:

1. In the future the agency should create a centralized cloud center that outlines the responsibilities of THECB and cloud vendors, an inventory of each cloud product, baseline security configurations, policies and procedures, and internal control documentation in accordance with NIST 800-53 Configuration Management controls.
2. Add the DMI deliverables to established annual risk assessments initiatives in accordance with agency risk assessment policies and industry standard frameworks such as NIST 800-53 Risk Assessment controls.
3. Ensure adequate staffing in key information security roles through active recruiting and ensure ongoing training for current staff.

Management Actions In Progress March 2022

- Recommendation One:
  - Management Action: The security team has adopted the NIST 800-171 system security plan (SSP) to describe the controls that are in place in each cloud-based system for meeting the applicable security requirements. SSP also delineates responsibilities and expected behavior of all individuals who access the systems to protect agency information. Security is in the process of selecting a tool to implement a centralized repository of the cloud resources owned by the agency. This task has been added to the FY22 Key Security Initiatives Implementation Roadmap and is expected to be completed by June 2022.
- Recommendation Two:
  - Management Action: Each DMI deliverable, once it gets promoted into production, will be added to the scope of the existing annual risk assessment exercise.
- Recommendation Three:
  - Management Action: Effective 3/1/2022 Miguel Olivas has been appointed as the agency Information Security Officer (ISO). The ISO and the CIO are currently working with HR on the job posting to try to fill the vacant Security Analyst position. The ISS team currently has subscriptions to Pluralsight (an online platform that offers video training courses for IT professionals), Microsoft Premium Support, and a variety of training resources and webinars offered by the DIR. The ISO and the CIO expect the funding for these training opportunities will continue and will ensure ongoing training for all the existing staff on the ISS team.

Appendix I: Advisory/Nonaudit Services

- The IA Audit Plan, notifications, and updates serve as our agreement of services.
- In accordance with auditing standards, IA cannot make management decisions. For example, we cannot create policies and procedures for program staff.
- IA reserves the right to audit areas previously reviewed as advisory or nonaudit services.
- Project scopes, objectives, and methodology are subject to change.
- Management assumes responsibility for addressing issues and risks.
- IA will perform follow-up verification on significant issues and risks.
- Internal Auditors have no direct operational responsibility or authority; which is covered extensively in our charter.

Thank you to Information Solutions and Services (ISS) and Data Analytics and Innovation for their ongoing support and resources on this project.

THECB Texas Higher Education COORDINATING BOARD

9

9

Texas Higher Education
COORDINATING BOARD

Questions?

10