DATE: 19 July 2013

TO: Chief Executive Officers
    Chief Financial Officers
    Executive Committee

FROM: Mark A. Stone
    System Chief Information Officer

RE: Deloitte Future State Recommendations — Part 1 Executive Summary

A Comprehensive IT Assessment was initiated by The Texas A&M University System to gain System-level insight into multiple facets of the IT environment across all Member Institutions and Agencies, and to develop a System-level set of recommendations designed to increase the effectiveness and efficiency of the System. This *Future State Recommendations—Part 1 Executive Summary* provides a description of a set of recommendations for TAMUS intended to lay a solid foundation upon which to develop, grow and innovate in the process of becoming a “world class” Information Technology organization. Core to this foundation are the principles of reducing risk, exercising fiduciary control, building trust and a sense of “System” among Members, and developing strong leadership at both the System and System Member levels.

The specific purpose of the *Future State Recommendations—Part 1 Executive Summary* is to provide a brief description of the 14 recommendations that will strengthen IT leadership, reduce risk, and/or improve operational efficiency for the following focus areas across all 22 in-scope System Member Institutions and Agencies.

- **Information Technology Governance** — IT Governance includes evaluating who is responsible and accountable for making and executing IT decisions and how these decisions are made, communicated and monitored
- **Information Technology Security** — IT Security includes assessing how well sensitive information and IT resources are secured and protected
- **Information Technology Network and Infrastructure** — IT Network and Infrastructure includes review of IT policies and standards, networking capabilities, and existing infrastructure architecture

The following is a list of the recommendations in this document.
IT Governance
- Recommendation 1: Reduce risk and increase leadership capability by establishing key System-level IT strategic roles
- Recommendation 2: Reduce risk, enhance trust and collaboration, and improve IT strategic alignment with comprehensive IT governance
- Recommendation 3: Improve efficiency and reduce cost by delivering in-common IT capabilities in a shared services model System-wide
- Recommendation 4: Reduce risk and increase consistency by establishing a comprehensive IT governance framework for System Members
- Recommendation 5: Reduce costs and improve efficiency through strategic sourcing for IT procurements

IT Security
- Recommendation 6: Enhance information asset protection and efficiency with a comprehensive Information Security Program and defined security roles across the System
- Recommendation 7: Increase effectiveness and reliability of IT Security via utilization of a common risk-based approach to assessments, and associated proactive monitoring
- Recommendation 8: Increase the level of incident response with a System-wide Cyber Security monitoring and reporting strategy
- Recommendation 9: Reduce risk through proactive implementation of Strategic Security Technologies and enhancement of data protection capabilities

IT Network and Infrastructure
- Recommendation 10: Reduce risk and improve efficiency by consolidating data centers to Tier-3 facilities
- Recommendation 11: Drive additional cost reductions and lower risk through the standardization of System-wide virtualization and further consolidation of servers and storage
- Recommendation 12: Increase efficiency and flexibility by using cloud resources
- Recommendation 13: Increase research wins by deploying a new research data hosting capability
- Recommendation 14: Achieve lower costs and higher reliability by adopting a cloud-hosted email solution

Attached you will find a complete copy of the Future State Recommendations – Part 1 Executive Summary. Upon your completed review, you should provide copies of this summary to your technology leaders.

In that Deloitte is currently completing the field work for Part 2 of the Future State Recommendations, member institutions and agencies are not being asked to undertake any projects or initiatives at this time. When both parts of the future state recommendations are released, these recommendations will provide an explanation of future system-wide efforts and serve as a tool in making member institution/agency technology decisions.

If you have any questions regarding the use of this summary, please contact me at 979-458-6440.
implement enterprise-wide policies e.g. data security standards, leading practices, etc. PIs will then be able to focus on their core competency – research – and enlist the support of the hosted cloud based research services for quick set-up and management of their IT environment. Also, providing services that meet the data management and dissemination requirements makes it simpler for PIs to complete data management plans that are required as a standard part of many grant proposals.

**Recommendation 14: Achieve lower costs and higher reliability by adopting a cloud-hosted email solution**

Email as a service (cloud hosted email) is experiencing rapid growth among educational institutions, with some projections showing it as the dominant model for University student populations by 2015. Particularly popular are the no-fee email offerings which feature self-serve administration for users and a variety of options for mobile technology, making them very popular with students.

![Figure 6: Student Email Systems](image)

**Source:** Gartner (10 Dec 2010)

Email as a service as an icebreaker, The Email Sourcing Trend in Higher Education, 2006 to 2012

There are a number of major cost advantages by adopting cloud-based email services. Because cloud services utilize vendor infrastructure for compute and storage resources, the costs of servers, storage and licenses to host email services are eliminated. And because these types of email services typically provide extensive self-serve administration tools, the costs of support are also greatly reduced.

Cloud hosted email systems are typically much more reliable than locally hosted systems, (support uptime is generally 99.9% or better) with enhanced security features. Additionally, cloud hosted systems employ aggressive spam filtering features and have extensive security controls as well.

TAMUS currently has twelve email systems for students and twenty-four email systems for its staff and faculty. As many of these systems are locally administrated, the operational and support staff is replicated across many locations. In many cases, the email offerings available to various users are highly duplicative with no major service distinctions between the various products.

TAMUS can reduce costs of its email services by reducing from thirty-six offerings down to two primary classes of service for email. The initial focus should be on taking advantage of the no-fee, email as a
service offerings for students. Further gains may be possible by moving additional email users, such as faculty, to cloud services.

Note: Some TAMUS Members are currently using email as a service products. However, the products being selected are varied and there are a substantial number of students that are being hosted on locally administered platforms.

2.3 Where To Go Next

The Part 1 Future State Recommendations focus on putting in place the foundation on which TAMUS can build a Top 10 IT environment. The recommendations presented were chosen because they were identified as the ones which provide the most value to TAMUS. The value these recommendations bring is measured in several ways, including risk reduction, cost savings, and/or research enablement. In addition to these initial recommendations, there are several other areas in which opportunities may be found. As an on-going process, the System should continually identify potential recommendations for analysis and implementation as additional avenues to differentiate itself as a Top 10 research, teaching and outreach System. As a starting point, once the foundation has been established, TAMUS should consider the following potential initiatives:

- Consolidate voice/video technologies, deploy VoIP to all System Members, and provide for virtualized phones (soft phones) to reduce telecommunications costs and improve consistency of services. This should be considered as a part of an enterprise wide converged network strategy. Specifically, leading practices indicate that TAMU should not continue to build out new facilities with separate data and voice networks, but instead should build out a converged campus network. This will allow the System to reduce operational costs, decrease design and integration complexity, increase deployment and support efficiencies, and increase network performance.

- Standardize provisioned network services at remote sites, ensuring redundant links and diverse paths to support improved continuity of service and disaster recovery

- Develop and implement a standard model for single sign-on (SSO) across the system using a Federated approach to identity management

- Create a Learning Management System shared service as part of the IT Shared Services organization at the System level

- Develop a System-wide approach for Open Learning, initially targeted at non-degree, non-certificate-granting programs

- Similar to Texas A&M University – Galveston and Tarleton State University, the System should consider streamlining internal operations by outsourcing all residential facility networks (e.g. WiFi, network connections in residence halls, etc.) that are currently managed by TAMUS organizations to a qualified, proven third party provider. As a result, the System will be in a position to reap many short term and long term benefits including reduced network maintenance and support costs, increased TAMUS network performance as a result of reducing / eliminating student data load (e.g. entertainment activity) off of existing campus networks, and reduced digital rights management and data content risk as a result of shifting all student residential network traffic off TAMUS-owned networks