Comprehensive IT Assessment
Future State Recommendations – Part 1
Executive Summary

June 2013
1 Background

1.1 Purpose
This Comprehensive IT Assessment was initiated by the Texas A&M University System (hereinafter referred to as either, “TAMUS,” or “the 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. While performing this assessment we have met with many talented, dedicated individuals, including many who regularly go “above and beyond” to ensure the best environment for those they serve. We have found organizations, or parts of organizations, that are doing many things very well, and who have developed strategic plans to guide their efforts. We have also found many opportunities for improvements and efficiencies throughout the System. This Part 1 Future State Recommendations 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 first part of this foundation will be the establishment of a strong IT governance and leadership model led by a System CIO. The second part of this foundation will be a strong security model which will provide the appropriate controls necessary for the System (and its Members and Board of Regents) to exercise all proper fiduciary responsibilities. The final part of this foundation will be a central, independent IT shared services (ITSS) organization that will deliver common services in an efficient and effective manner, while reducing System-wide costs.

1.2 Purpose of This Document
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 (See Table 1, below, for a complete listing).

- **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
1.3 Basis for These Recommendations

These recommendations are based on the Data Gathering and Current State Analysis activities conducted by the Deloitte team, during which information was gathered and analyzed from each individual System Member. It is also based on Deloitte’s experience on projects of similar size, scope and complexity, and on benchmarking data for comparable work done within higher education and other public sector and commercial industry segments. The TAMUS data gathered and analyzed gave us a critical understanding of how IT is delivered across the System today, identified a number of internal leading practices currently in place, and uncovered several potential improvement opportunities for the System. Deloitte experience and peer benchmarking was then used to apply leading practice examples to the TAMUS environment, resulting in the set of recommendations presented in this report.

The detailed data collection effort began in the first week of December 2012 and concluded in the third week of February 2013, with some additional follow-up continuing through the date of this report. This data collection effort spanned all 22 in-scope Member Institutions and Agencies, including the System Office itself. The data collection effort included:

- A tailored questionnaire distributed to all 22 in-scope Member Institutions and Agencies
- A tailored document request list distributed to all 22 in-scope Member Institutions and Agencies
- A set of formal interviews with all 22 in-scope Member Institutions and Agencies, in which a total of 185 executive and operational leaders participated
- Physical tours of 19 data centers, facilities, and campuses

The data gathered through each of these methods was validated with System Members and was then reviewed and analyzed by the Deloitte team. The intent of the initial analysis activities was to create a substantially complete view of IT Governance, IT Security, and IT Network and Infrastructure, identifying key themes in each of these three areas of focus.
An additional analysis effort was then conducted after the data gathering and synthesis period. The goal of this analysis was to identify specific, actionable recommendations to be made to TAMUS. The data and information collected across the System served as a starting point for this analysis, in that it provided an understanding of the System as a whole, as well as for each individual System Member to some extent. This initial understanding of TAMUS was then compared with a proposed vision of what IT would look like at a “Top 10 Research, Teaching, and Outreach” System. Where there were gaps, recommendations were formed that would bridge those gaps. Both experience (in higher education, public sector, and the commercial sector) and comparable trends informed this analysis and, as such, underpin these recommendations.

1.4 Summary of Part 1 Future State Recommendations
The following is a list of the recommendations included in Section 4 of 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
2 Future State Overview

The Future State Guiding Principles described below constitute the basis for our Future State Vision and the specific recommendations described in this executive summary that will provide the foundation for implementing this Vision. These Guiding Principles were developed based upon Deloitte’s understanding of TAMUS’ goals and objectives for this Comprehensive IT Assessment and for System IT overall. The Principles provided a framework for defining a Future State Vision of IT across the System, described below, and, as such, served to guide the development of specific, executable recommendations that will enable the System to achieve this Vision.

2.1 Future State Overview

2.1.1 Future State Guiding Principles

- **System-wide Focus.** The System Office should provide strong leadership across all System Members, through both executive roles and well-understood governance processes and structures. This leadership focus should recognize not only the mission of the System, but also of each System Member, whether Institution or Agency.

- **Cost Control Using a Balanced Value Focus.** Make better use of scarce resources to support teaching and research activities core to TAMUS’ mission. Decisions to adopt or defer new ideas, technologies, standards, or initiatives should be informed not only on the total cost of ownership (TCO), but also by reduction of risk (or improvement of ability to meet fiduciary responsibilities), added business value, improved operations and user experience, and standards compliance/harmony.

- **IT Security Focus.** IT should ensure that all System Members are properly equipped to provide appropriate levels of security to all faculty, staff, students, visitors and other users at all times.

- **Customer-driven Service Focus.** Services provided by the System Office or associated shared service-focused System Members should address the business needs and requirements of the customers they serve.

2.1.2 Future State Vision

The Texas A&M University System of the future will be included in the top tier of research, teaching and outreach systems globally. As such, the System will have the following IT attributes providing the continuing foundation on which that top tier global status was built and will be maintained.

- Strong leadership at the top and across all layers that enables the core mission of the System
- Effective governance across the System that promotes collaboration and innovation
- A System-wide information security strategy that ensures that people, process and technology will proactively and efficiently provide for the confidentiality, integrity and availability of information assets, that significantly reduces risks, and that enables alignment with regulatory requirements
- Minimal System Member-hosted data and applications that are critical to the missions and unique business needs of individual Member Institutions/Agencies
- A shared service framework that provides a foundation for common services
2.2 Phase 1 – 3 Recommendation Summaries

The set of recommendations summarized below provides a framework for establishing this foundation described above, and raising the level of IT at TAMUS.

2.2.1 IT Governance Recommendations

To achieve the desired IT governance vision, the System should embark upon a series of initiatives that, over time, will:

- Provide strong IT leadership and an IT voice in strategic decision-making across the System
- Strengthen and mature IT governance at the System level and across Member Institutions/Agencies
- Lay the foundation for collaboration and the recognition of economies of scale amongst System Members

**Recommendation 1: Reduce risk and increase leadership capability by establishing key System-level IT strategic roles**

Establish position descriptions for and hire a permanent, full-time, independent System Chief Information Officer (SCIO) and Chief Information Security Officer (CISO). Consider also appointing at some point in the future a Chief Data Officer (CDO). Establishing these roles within the System Office and with oversight responsibility for the System as a whole will allow for the development of a System-wide IT strategic vision and IT security program that can then be carried out at each of the System Members.

**System Chief Information Officer**

The SCIO will be responsible for formalizing and managing System-level IT strategy, aligning IT strategy with System-wide business objectives and strategy, developing and managing System level IT standards, promoting technology innovation, advising on the direction of IT services to be offered System-wide, and actively leading the IT community across the System. The SCIO will report directly to the Chancellor and will sit on the Executive Committee. For further detail on the recommended role of the SCIO within the recommended IT governance structure, see Recommendation 2.

**Chief Information Security Officer**

The CISO will be responsible for establishing and maintaining a vision, strategy, and program for the protection of the System’s information assets, setting security standards and policies, advising on the direction of security services to be offered System-wide, and providing strategic direction to risk management and security initiatives at the System level and at the System Member level. For further detail on the role of the CISO in the IT governance structure, see Recommendation 2. For further information on the role of the CISO in establishing a System-wide security program, see Recommendation 6.

**Chief Data Officer**

Once the SCIO and CISO have been on-boarded, the System should consider adding a CDO to provide specific strategic leadership focus on data as a valuable System resource. The CDO would be responsible for driving data quality and consistency to meet business needs, enabling cross-System data sharing, and setting System-wide data standards and report requirements for the collection, delivery and use of data and associated systems. For example, the CDO would be instrumental in facilitating cutting-edge and timely reporting for the increasing number of research programs that are managing large data sets (e.g.,
Recommendation 2: Reduce risk, enhance trust and collaboration, and improve IT strategic alignment with comprehensive IT governance

Develop and implement a comprehensive System-wide IT governance structure, consisting of an IT Governance Board responsible to the Chancellor, Executive Committee, and a number of standing sub-committees. In addition to the IT Governance Board, establish a number of Communities of Practice to provide System Members with forums for information sharing and exchanging ideas and potential solutions to common problems. This structure will provide a collaborative mechanism for the System and its Members to address System-wide and regional IT priorities, align these priorities to the System-wide strategic direction, have a voice in IT decision-making at the highest level, and stay continually connected to their IT colleagues across the System on a range of relevant IT topics. Each governing body will have a clear charge and direction on its agenda, the types of decisions it is responsible for making or advising on, how decisions are made and implemented, and how progress is to be monitored and reported on. System-level policies will be used to formalize these IT governance groups. Both the IT Governance Board and the Communities of Practice will be described in more detail below, and a recommended IT Governance structure and the responsibilities of each level are depicted in Figure 1.

IT Governance Board

The IT governance structure will address the current IT governance gap at the System-level by establishing a single IT Governance Board comprised of business and IT leaders to provide customer input and subject matter expertise into the strategy and operations of IT across the System. This IT Governance Board will be responsible for making recommendations and providing operational reviews to the Chancellor and Executive Committee on IT strategic investments, the System-wide IT portfolio of services, IT policy, and IT standards. Ultimately, the Chancellor will be responsible for making decisions based on these recommendations. The primary focus of the Board will be to achieve System-wide business and IT alignment.

It is recommended that the IT Governance Board be co-chaired by the SCIO and the Vice Chancellor for Academic Affairs, and include both IT and business representation from System Members to ensure that IT recommendations are made with joint business and IT input and align to both System-wide and Member-centric missions and strategic goals.

Membership on the IT Governance Board will be comprised of the SCIO, members of the Executive Committee designated by the Chancellor, and nine System Member business and IT representatives who serve staggered three-year terms on the Board. Representation will rotate between System Members and between IT and business members, keeping a representative mix of System Members and a relatively even split between IT and business. Membership will be voted on by System Members, with the precise mechanism for selection being decided upon during implementation working sessions with a broad group of executive stakeholders to be defined by the Chancellor or his designee(s).

IT Governance Board Sub-committees

The IT Governance Board will have several standing sub-committees that will focus on specific IT domains. Membership on these sub-committees will be comprised of a designated Chair, three rotating System Member IT Governance Board representatives, and 1-2 additional standing members from the IT Governance Board. Recommended sub-committees include:

petabytes). This strategic role would work closely with the CISO on data security and privacy, setting standards and guidelines related to who owns what data and how it is protected.
• IT Services – Chaired by the SCIO and responsible for guiding the portfolio of IT shared services, associated service levels, key performance indicators, and assessment methodologies (see Recommendation 3 for further detail on IT shared services)

• Security and Privacy – Chaired by the CISO and responsible for providing overall leadership and direction for the Information Security Program, ensuring coordination and compliance with privacy regulations, and mandating compliance with the System’s information security policies and practices (see Recommendation 6 for further information on the System-level Information Security governance structure)

• Research Enablement – Chaired by the Executive Director of Office of Sponsor Research Services and responsible for overseeing all technology-based services that underpin the System’s ability to conduct research, initially including the proposed Research Data Hosting service (see Recommendation 13 for further information)

Communities of Practice

In addition to the IT Governance Board and sub-committees, the recommended IT governance structure proposes the inclusion of a number of cross-Member collaboration groups organized as Communities of Practice (CoP). A CoP is a group of individuals bound together by a common area of specialization, focused on sharing knowledge with each other, developing potential solution approaches to problems with broad applicability, and disseminating information throughout the organizational units represented by the individuals. CoPs will often also take on additional roles when operating in a more formal environment. For example, these proposed CoPs will provide operational reviews to sponsoring executives, as described below.

It is recommended that a number of existing cross-Member forums be re-shaped and formalized into CoPs under this structure, including the CIO Council and ISO Working Group. In addition, it is recommended that the System stand up CoPs focused on applications and infrastructure. The System may consider adding additional CoPs in the future to meet the specific needs of System Members.

CoP membership is voluntary, though all System Members will be encouraged to provide appropriate representation to ensure the highest level of communication among members and to encourage the exchange of knowledge and leading practices. A CoP chair, or co-chairs, will be appointed for 2-year terms.
Recommendation 3: Improve efficiency and reduce cost by delivering in-common IT capabilities in a shared services model System-wide

Migrate to an IT Shared Services (ITSS) model. This model (whether it is one member institution providing services for another, services consolidated at the System Office, or a new Member responsible for the management and delivery of IT services available to all System Members) will reduce IT redundancy for commonly used software and services, provide consistency in the IT services delivered across the System, and make specific IT expertise for services within the ITSS portfolio available to all System Members. This model will also provide a mechanism for capturing System Member input and requirements related to the services provided and develop potential new services as needed. One of these mechanisms will be the creation of a business engagement position responsible for liaising between the ITSS function and its Members, both to advocate for Member needs and to inform Members of what is possible and what the potential solutions are.

The mission of ITSS operations will be focused on responsive and business-justified IT service delivery and cost-effective IT operations management. The primary responsibilities of ITSS operations will include:

- Managing IT services provided System-wide through an ITSS solution where cost and processes are justified
- Developing and maintaining performance management metrics for the IT services offered
- Developing System-wide Key Performance Indicators (KPIs) for IT services offered by ITSS operations that may also be delivered locally by System Members to promote consistency in service delivery
- Provide a mechanism for capturing and addressing System Member requirements for services offered by ITSS operations, as well as input into potential new service offerings
- Manage demand for services offered
ITSS operations will be funded by assessing System Members for the services they use. It is recommended that the System consider bringing certain IT services that are currently provided to all System Members, such as TTVN, FAMIS, BPP, etc., into a System ITSS operation. Additional due diligence will be required to determine what specific existing services will be migrated to an ITSS operation (some of which will be conducted during Part 2 of the Comprehensive IT Assessment). The schedule for transitioning each of these services will be determined by the Working Group, in consultation with executive System leadership, the executives currently responsible for each service, and System Members. It is also recommended that at the onset, certain new services be offered through a System ITSS operation, including certain IT security services (see Recommendation 6 for more detail) and data center hosting services (see Recommendations 10, 11, and 12 for more detail). The System should then consider adding additional IT services based on System-wide needs, cost justification and strategic priorities.

ITSS operations will be run by a senior IT leader (this could be one of the System Member CIOs initially, an existing resource, or a new resource), who will have operational responsibility for the services delivered. Typical job responsibilities for the senior IT leader will include developing a Service Level Agreement (SLA) framework and maintaining SLAs for each IT service delivered by the ITSS operation, developing a service catalog to communicate service offerings to System Members, and developing short and long term IT investment/savings plans for the ITSS operation. The senior IT leader of an ITSS operation will normally report to the System CIO (unless the ITSS operation logically should report to one of the System Members) and will work in close collaboration with both the CISO and System Member CIOs on the specific technology and security services offered to ensure that IT service delivery is aligned with the overall IT strategic vision and security program of the System. In addition, it is recommended that a Business Engagement role (may also be an existing person initially), as mentioned above (reporting to the senior leader of an ITSS operation), be responsible for liaising between the ITSS operation and System Members in regards to satisfaction with the services offered, change requests for current services, and requirements for new services. Figure 2 illustrates this organizational structure.
Figure 2: ITSS Executive Director Reporting Structure

The IT Services Sub-committee of the IT Governance Board will be responsible for overseeing the portfolio of services offered by ITSS operations, approving Key Performance Indicators (KPIs) and specific service levels for each service, and developing the methodologies to be used for assessing System Members for each service.

Recommendation 4: Reduce risk and increase consistency by establishing a comprehensive IT governance framework for System Members

Establish an IT Governance framework that will provide guidance to System Members as they develop and strengthen the IT governance structures at their Institutions/Agencies. By aligning this framework with the System-wide structure implemented through Recommendation 2 and building on the leading IT governance practices at many System Members already, this framework will provide consistent processes, tools and templates for the execution of effective IT governance System-wide. The framework will also provide a mechanism for building a collective sense of System among Institutions/Agencies, as they begin to align strategic planning processes, leverage leading practices from one another, and work toward elevating the role of IT to that of a strategic partner across the System.

IT Governance Framework Overview

The goal of the IT governance framework is to provide System Members with a primary source of information on IT governance at the System Member-level with a focus on the following areas:

- IT governance definition
Guidance on structuring IT governance bodies and defining roles, responsibilities, and membership of these bodies, including a mix of business and IT representatives

Guidance on developing charters for these IT governance bodies

Proposed processes for interacting with executive leadership, other governing bodies, IT and the business, which can then be tailored by the specific needs and structures of each Member Institution/Agency

Proposed processes for selecting members, making decisions/recommendations, strategic planning, and other key activities, which can then be tailored by the specific needs and structures of each Member Institution/Agency

The IT governance framework will not be a guide for managing IT – it will not be prescriptive in defining IT operating models, organizational structures, staff reporting relationships, or span of control. Rather, the framework will define the critical components of IT governance in a manner that can be leveraged as a reference guide and tailored to the specifics of each System Member’s Institution/Agency. The key objectives of the IT governance framework will be to:

Provide tangible materials for System Members to leverage in improving their IT governance, regardless of its current maturity

Provide leading practices from within the System currently and from higher education and other industries more broadly on how to best structure and maintain transparent and effective IT governance

Provide guidance and lessons learned on how to accomplish basic IT governance responsibilities such as aligning IT with the business, strategic planning, monitoring and reporting, managing IT investments and project portfolios, overseeing risk management and reduction, and ensuring the responsible use of IT resources

**IT Governance Framework Ownership and Management**

The IT governance framework will be developed by a Working Group comprised of System Member IT and business representatives under the sponsorship of the SCIO and with input from the CISO, other System-level executive leaders, and System Member executive leaders. Once drafted, the IT governance framework should be reviewed by the CIO Council and socialized among business and IT stakeholders across all System Members for input and feedback prior to finalization and distribution. Ownership and management of the IT governance framework should then reside with the CIO Council under its new structure as a Community of Practice (CoP). This CoP will be closely supported and advised by the SCIO and, as such, the CoP can ensure continued alignment between System Member IT governance and System-level IT governance. The CoP will also implement a process for the continued review and improvement of IT governance System-wide, which will then be fed back into the IT governance framework.

**Recommendation 5: Reduce costs and improve efficiency through strategic sourcing for IT procurements**

Develop a detailed plan working with TAMUS System Member IT and procurement leadership to analyze current and historical IT spend and procurement processes across all System Members to identify System-wide trends by product and vendor type and identify leading practices for procurement processes. This will allow the System to:

Develop System-wide standards and guidelines for the procurement of software, hardware and commercial off-the-shelf (COTS) products
• Identify opportunities to develop IT strategic sourcing relationships with targeted vendors
• Maximize the purchasing power of the full System
• Streamline IT procurement processes at the System Member-level
• Identify potential revisions to System-level IT procurement policies

The plan should identify opportunities for the System to leverage its size and reputation, align and consolidate vendor contracts, and share information about products and services in order to achieve better pricing on the products and services that all System Members are currently buying independently. It will also improve the efficiency of the IT procurement process by identifying strategic vendors and developing procurement standards and guidelines that all System Members can follow without spending excess time researching potential solutions and negotiating with vendors independently. Improved IT procurement policies and the introduction of standards and guidelines will improve System-level visibility into IT spend across the System, allowing the System to better track and monitor IT spend on an ongoing basis, and will allow the System to continually rationalize its supplier list and build more strategic relationships with a targeted list of high-quality vendors.

2.2.2 IT Security Recommendations

A system-wide information security strategy will ensure that people, processes and technology proactively and efficiently provide for the confidentiality, integrity, reliability and availability of all of the System’s information assets in support of the attainment of business objectives and the System’s Board of Regents fiduciary responsibility to its constituents.

In order to achieve these objectives, the System should evaluate the security recommendations laid out below in light of the following themes:

• Secure information assets by aligning the Information Security Program with the System’s business objectives using a balanced, cost-effective, business-based approach
• Protect information assets and respond to security incidents in a timely manner by monitoring and reporting System-wide security performance and compliance to assess the effectiveness and efficiency of the Information Security Program
• Increase efficiency of execution via defined security roles and responsibilities between System Office and all System Members
• Increase effectiveness and reliability of information security through improved daily operations management, utilization of a common risk-based approach to security assessments, and proactive monitoring of vendor and 3rd party relationships
• Proactively define and implement strategic security technologies resulting in the creation of a leading-edge security infrastructure to which applications and services are integrated enhancing the System’s capability to proactively react to security risks
• Enhance consistency and quality of execution via standardized security architectures and well documented security policies and technology standards.
Recommendation 6: Enhance information asset protection and efficiency with a comprehensive Information Security Program and defined security roles across the System

TAMUS should establish a System-level information security governance structure that defines a System CISO function responsible for defining minimum security requirements, framework(s) to be adopted, and setting minimum expectations for System Members to follow. This function would be responsible and accountable for defining policies, security reporting, and monitoring System Member implementation.

To achieve the recommendation, the System should coordinate all security-related functions under the guidance of the CISO. The CISO should be strategically placed at the System level to ensure that information security initiatives receive the proper visibility and that they align with the System’s business objectives. The CISO would serve as the focal point for information security matters and, in conjunction with the existing Information Security Working Group (ISOWG), ensure the information security objectives are being achieved. (See Recommendation 1 for more details about the CISO position)

Figure 3: CISO Responsibilities

The information security program should also define a list of information security shared services that will benefit the System and System Members. The purpose of the shared services would be to provide System Members with an avenue to perform IT Security functions they may not otherwise implement for various reasons. For example, few System Members have a SIEM tool installed that logs and monitors security events due to human or financial resource constraints. This service would be one of several identified by the CISO that would provide benefit to TAMUS and may not be implemented otherwise by a System Member. (See recommendation 3 for more details).

Recommendation 7: Increase effectiveness and reliability of IT Security via utilization of a common risk-based approach to security risk management, and associated proactive monitoring

Each organization should be aware of their information security risks and risk tolerance to ensure critical information assets are safeguarded with the proper controls. TAMUS should implement a risk management approach that is based on a foundation of risk identification, risk assessment and risk management. This approach should establish an ongoing process that drives the System towards the most useful and cost-effective controls to mitigate security risks.

As a component to the risk management approach, third party risk management must be addressed to place the proper controls around third party vendors with access to sensitive data. The components of third party risk management should include a security risk and controls framework, a process for monitoring risks based upon classification, and an approach to evaluating high risk contracts.
Once developed, the approach should be implemented by System Members to ensure a uniform approach for risk management is followed throughout the System.

**Recommendation 8: Increase the level of incident response with a System-wide Cyber Security monitoring and reporting strategy**

Developing a standard approach to address cyber-threats and vulnerabilities would allow each System Member to deploy uniform minimum requirements for:

- **Vulnerability management**: Establish requirements to proactively identify and mitigate risks related to the potential exploitation of vulnerabilities in the environment
- **Logging and monitoring**: Establish baseline requirements for ongoing system security logging and monitoring for timely detection of, and response, to potential unauthorized or malicious activity
- **Incident Response**: Define and establish a common approach to incident response for the efficient identification, investigation and resolution of cyber-security incidents that will allow the System Members to respond to cyber-security incidents in a consistent manner

The successful implementation of these controls will increase TAMUS’ ability to proactively identify and respond to malicious cyber activity.

**Recommendation 9: Reduce risk through proactive implementation of Strategic Security Technologies and enhancement of data protection capabilities**

Data breaches of sensitive information may result in substantial financial penalties for the offending organization. As such, TAMUS should develop and implement a strategy for increasing the protection of sensitive information through deployment of data protection processes and technologies (such as DLP, encryption) as well as architecture (e.g., network segmentation). Within this strategy, minimum requirements for data protection and infrastructure security technologies will be defined to provide the System with adequate information security coverage in these areas.

The data protection strategy involves developing uniform procedural controls for data classification, establishing clear roles and responsibilities for data owners, and standard guidelines for network segmentation. Documenting and implementing these safeguards in a consistent manner throughout the System reduces the risk of sensitive data being stored, accessed, or transferred in an unsecure manner.

We also recommend that the System develop a set of minimum requirements for information security technologies tools deployed by each System Member. Establishing these technical standards will provide TAMUS with consistent, appropriate technical controls that will prevent, detect, and deter malicious activity on TAMUS networks. The successful implementation of this recommendation will reduce the risk of data leakage going undetected.

**2.2.3 IT Network and Infrastructure Recommendations**

For the Texas A&M University System to realize its vision as a Top 10 research, teaching and outreach System, it will need to be supported by Top 10 IT network and infrastructure services. As such, the System’s IT environment of the future will be:
Highly virtualized and built on an elastic demand model to enable fast growth, lower costs and promote nimble response to business needs.

Monitored and governed to move towards increased operational efficiencies and customer satisfaction by replacing local service and point-of-use systems with centrally managed IT shared services, providing service levels commensurate with business needs.

**Recommendation 10: Reduce risk and improve efficiency by consolidating data centers to Tier 3 facilities**

With a consolidated data center approach, TAMUS can make use of economies of scale by leveraging strategic sourcing and the buying power of the System. The consolidated data center approach will also promote uniform use of technologies, reduce audit compliance risk, and increase TAMUS’ ability to expand into new service offerings like research data hosting, System-wide colocation services, first class disaster recovery services, private cloud services, etc. This will be especially advantageous for smaller System Members which do not have the skillset or budget to build and maintain top tier IT infrastructure.

These Tier 3 data center facilities would offer a wide variety of hosting services including a best in class primary and disaster recovery (DR) site for mission critical applications and research data. These services should be tiered based on application criticality and requirements specified by each participating Member (e.g. Tier 2, Tier 3, Tier 4 in terms of availability and resiliency). See “Tier Level Classification” reference below for tier-specific information. Tier levels are defined by The Uptime Institute, a Santa Fe, New Mexico-based think tank and professional services organization.

### Tier Level Classification

- **Tier 4 (High Cost, High Service)**
  - Fulfills all Tier 1, Tier 2 and Tier 3 requirements
  - All cooling equipment is independently dual-powered, including chillers and Heating, Ventilating and Air Conditioning (HVAC) systems
  - Fault tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability (up to 26 minutes of annual downtime)

- **Tier 3**
  - Fulfills all Tier 1 & Tier 2 requirements
  - Multiple independent distribution paths serving the IT equipment
  - All IT equipment must be dual-powered and fully compatible with the topology of a site’s architecture
  - Concurrently maintainable site infrastructure guaranteeing 99.682% availability (up to 94 minutes of annual downtime)

- **Tier 2**
  - Fulfills all Tier 1 requirements
  - Redundant site infrastructure capacity components guaranteeing 99.741% availability (up to 23 hours of annual downtime)

- **Tier 1 (Low Cost, Low Service)**
  - Single non-redundant distribution path serving the IT equipment
  - Non-redundant capacity components
  - Basic site infrastructure guaranteeing 99.671% availability (up to 29 hours of annual downtime)

*Figure 4: Tier Level Definitions*
The hosted facilities and services provided should be designed based on the business, technical and security requirements confirmed by TAMUS leadership, and aligned with System and State audit standards. While top tier (Tier 3 and Tier 4), high availability services will be the primary service offering at these facilities, there will also be Tier 2 service offerings for applications that do not require high availability services. Moreover, tiered services should be offered at a competitive market price relative to other 3rd party and include official service level agreements.

Examples of potential services offered to System Members may include the following (but not limited to):

**General Services**
- Basic facilities infrastructure like floor space, power, cooling, storage, and network connections to/within the pod area. Some of these features should be offered at varying levels depending on the Member’s need. For example, high and medium availability, single and redundant cooling, high and medium bandwidth replication, etc.
- Secured physical access to the facility
- Uninterruptable power supply (UPS), battery backup and standby generator services
- 24 X 7 monitoring of environmental control systems
- Service level agreements (e.g. availability, recovery time objectives, etc.)
- Colocation space and cage
- Remote Admin access
- Various reporting capabilities (e.g. used and unused storage capacity, testing results, etc.)
- Climate detection sensors (e.g. water intrusion, temperature change, etc.)

**Disaster Recovery Services**
- Mirrored storage replication from the primary Tier 3 data center to the disaster recovery tier 3 data center (using high bandwidth connections)
- System backups (disk, tape) and snapshots
- Regular failover and recovery testing (automatic and manual failover). This service may include testing training and support
- Comprehensive DR plans
- Fire detection and suppression system

**Research Data Services (any and all services listed above could also be applied to hosted research data)**
- Sufficient power for all installed equipment with visual usage information
- High bandwidth network connections to the campus backbone and to the researcher-provided switch in the high performance computing cluster

**Private Cloud Services**
- Highly scalable, virtualized, and standardized data solutions controlled by TAMUS and offered over a private network, that enable on-demand provisioning (e.g. adding/reducing compute capacity upon business need)
• Software-as-a-Service (SaaS): Licensing an application to customers for use as a service on demand

• Infrastructure-as-a-service (IaaS): Offering computer infrastructure (typically a platform virtualization environment) as a service

• Platform-as-a-Service (PaaS): Building, delivering applications, services and computing platforms as a service

**Recommendation 11: Drive additional cost reductions and lower risk through standardization of System-wide virtualization and further consolidation of servers and storage**

Consolidation of servers and storage devices achieves savings by targeting and eliminating duplicative hardware and applications, replacing them with more efficient centralized systems. Consolidation reduces the amount of space required to host devices, the total power consumption, cooling costs and overall facilities costs. It also reduces the size of the operational teams required to support the devices.

Virtualization technology also reduces costs by enabling organizations to get more work out of devices. It intelligently distributes work across devices, allowing applications and users to share resource pools. This greatly reduces the number of idle devices in a data center while increasing the compute and storage density; thereby enabling organizations get the most out of data center square footage.

One additional benefit of virtualization technology is that it permits use of an elastic demand service model. Because virtual systems can be deployed quickly, wait times for new service are greatly reduced. And when services are no longer needed, the applications can very quickly be decommissioned, returning the resources to the shared pool.

Consolidation and virtualization would provide TAMUS with other benefits as well, including improvements of system reliability and uptime. Likewise, service quality benefits as more highly specialized staff support a narrowed range of products. This also has a beneficial impact on procurement functions as purchasing power is concentrated on a fewer number of models.

TAMUS does currently use virtualization technology. However, this technology is not well consolidated. Instead, most System Members are replicating the same technology in their data centers, driving up aggregate capital and operational costs across the System. Additionally, the current levels of device virtualization at TAMUS are below industry leading practice levels and substantial gains are still achievable. By both consolidating and further virtualizing its devices, TAMUS can significantly lower both operational and capital costs.

The virtualization and consolidation program would look intensively at current server and storage assets, assessing sizing, performance requirements and current workloads. It would use this information to identify assets for consolidation and virtualization, prioritizing the work based on potential savings to front end load savings for the project.

To further improve savings, server and storage devices would utilize classes of service aligned to the specific business requirements of the data and applications that support. Mission critical applications would be supported on fully redundant systems, allowing for premium features like automatic failover and full Disaster Recovery capabilities. Less critical systems would offer fewer features but would also have lower price points, allowing the business to determine the quality of service required.
The Program goals should be formalized in a roadmap that prioritizes tasks based on risk reductions, and cost savings to front end load benefits. TAMUS should also generate ongoing Program reports, which would provide metrics to allow for tightly controlled performance management.

**Recommendation 12: Increase efficiency and flexibility by using cloud resources**

Cloud services, both public and private, enable organizations to reduce capital and operational IT costs, improve data accessibility, increase quality of service, and meet elastic demands in a timely manner. The elastic nature of the cloud allows organizations not only to deploy and relinquish services quickly (e.g. software as a service, infrastructure as a service, storage as a service, etc.), but also pay for only the services used (i.e. “pay as you go” financial model). There is a large opportunity for TAMUS to reap these types of benefits in the near future while simultaneously meeting or exceeding System Member business, technical and security requirements. For instance, public cloud providers (Google, Amazon, etc.) offer application and data hosting services which could be made available to TAMUS, via web service, with varying degrees of privacy control. See additional sample examples of cloud vendors below.

![Figure 5: Sample of Cloud Vendors](image)

Non-sensitive TAMUS applications and data (e.g. student email and service desk applications) could be migrated to the cloud provider’s hardware and infrastructure, thereby alleviating TAMUS of day to day operations and maintenance management. TAMUS resources would then have the ability to focus on more value-add IT work like new development and innovation, which may lead to new opportunities and attract new talent to the System.

Depending on State or University legal standards and policies, there may be some restrictions on hosting data on public cloud infrastructure (e.g. specific research data, high performance computing data, etc.). This type of data could be hosted on a TAMUS private cloud service. A TAMUS private cloud would offer similar
benefits of a public cloud provider (e.g. flexible scalability advantages, storage on demand, paying only for services used, etc.). However, TAMUS would have to allocate additional funds to standup and manage this private cloud service because the private cloud services would be hosted behind the TAMUS firewall, managed by TAMUS resources, and hosted on TAMUS hardware. And while the initial startup costs may require a significant investment, the private cloud’s shared virtualized computing model would lay the foundation for substantial long-term benefits.

Some System Members have already migrated services to public and private cloud providers and reported positive results. For example, Texas A&M University - Kingsville and Tarleton State University are using Microsoft for student email services, and Texas A&M University has built a private cloud for the College of Engineering. However, a System-wide private cloud and a System-wide partnership with a public cloud service provider do not currently exist. Both options could benefit the System tremendously in terms of cost, scalability, security and quality of service. Moreover, rapidly changing technology standards and practices are driving many organizations to consider cloud computing as a viable alternative. TAMUS is currently in a position to adopt this trend on a large scale, and should consider investing in these options in the near future.

**Recommendation 13: Increase research wins by deploying a new Research Data Hosting capability**

A cloud based centrally managed research hosting service would provide superior hosting capabilities that can serve the computational power and storage needs of complex research projects across all TAMUS Members. This service offering also has the potential to increase collaboration between Principal Investigators (PIs) across TAMUS, reducing duplication and better utilizing expertise across the System, raising the potential to more effectively compete for large, multi-disciplinary grants.

Currently TAMUS has numerous hosted systems that support Research, many of which are bound by the physical limitations of the data center. Centralized, on demand capacity for research data storage is not available and the ability to attract and retain research grants may be impacted by the lack of availability and the quality of service offered. Large world class research organizations typically need secure storage and computing power services to launch and complete their research projects. Such organizations usually address capacity on demand for core needs such as server capacity, storage and telecommunications.

Principal Investigators (PIs) are increasingly relying on information technology to carry out research. The research data hosting services offering would provide a centrally managed, secure and reliable environment for hosting research data. These services would also meet data management and dissemination requirements as articulated by major grant providers and government agencies like the National Science Foundation (NSF).

To be a compelling hosting choice, the research data hosting services offering would be provided at a competitive price taking into consideration market pricing for similar sets of services. This would provide services at reasonable price points to PIs in support of putting their research environments in place via on-demand, hosted services.

Centrally managing this service offering would help realize increased efficiencies by leveraging similar IT services and infrastructure. This would also enable the standardization of processes and make it easier to
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](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