

LEGACY SYSTEMS STUDY

Assessment and Recommendations

PUBLIC REPORT



Texas Department of Information Resources
October 1, 2014

Contents

Executive Summary.....	1
Project Objectives.....	1
Analysis Approach	2
Assessment Results	2
Recommendations.....	3
High-Level Findings	6
Architecture Analysis	6
Mission-Critical Applications	6
Hardware and Software Components by Primary Functional Category	7
Legacy Remediation Cost Estimate	8
Average Age of Hardware Components.....	8
Recommendation 1	
Determine the Impact of Identified Security Risks and Prioritize Mitigation.....	9
Recommendation 2	
Develop a Legacy Modernization Roadmap Strategy	9
Recommendation 3	
Leverage DIR to Establish a Statewide Application Development Framework, Standardization and Consolidation	10
Recommendation 4	
Seek Commercial Off-the-Shelf Solutions over Custom-Developed Solutions.....	12
Recommendation 5	
Consolidate Reporting and Analytics into Consolidated Business Intelligence Services	12
Recommendation 6	
Implement Application Portfolio Management Practices	13
Appendix	
Functional Category Definitions	15

Legacy Systems Study
DIR Enterprise Solution Services
legacy.study@dir.texas.gov

Texas Department of Information Resources
300 West 15th Street, Austin, TX 78711-3563
www.dir.texas.gov

Executive Summary

Texas is a diverse state—from the geography of the landscape to the people who live here—and the needs of state agency systems to serve the public are just as diverse. As electronic records and online transactions increasingly become the standard for state government operations and statewide service delivery, it becomes more critical to understand the investment in and management of the supporting information systems.

The Legacy System Study (LSS) was created by the 83rd Legislature ([House Bill 2738](#)) to evaluate the composition of the state’s current technology landscape and determine how best to approach and make decisions about an aging infrastructure. A legacy system is defined in statute as a computer system or application program that is operated with obsolete or inefficient hardware or software technology.

Much like the physical infrastructure of public bridges and roads, the information technology (IT) infrastructure must be maintained to ensure continuity of service to the public. Aging systems that are either costly or inefficient in operations, or which simply do not have manufacturer support for the software, need prioritized attention.

This report offers a snapshot of current State of Texas legacy systems, along with recommendations for possible solutions to this critical and timely issue.

The Texas Department of Information Resources (DIR) was directed by the state legislature to perform a study detailing the use of legacy systems and software by state agencies (excluding institutions of higher education and agencies that are statutorily exempt from reporting information to DIR).

DIR’s Enterprise Solutions Services (ESS) team worked collaboratively with the legislatively specified agencies throughout the process to carry out the study in the following four phases:

- 1. Strategize**—Analyze House Bill 2738, then formulate a plan to collect data and report to state leadership
- 2. Gather**—Develop a data dictionary for consistency and assist the agencies in gathering data
- 3. Analyze**—Validate and analyze the data submissions, then formulate recommendations
- 4. Report**—Develop an assessment report and identify high-value remediation targets with estimates of costs

DIR completed the first two phases. To complete the final two phases, DIR partnered with a major international technology advisory company to ensure broad technology expertise in performing the analysis and reporting. The project team—made up of representatives from both parties—employed proven frameworks and methodology for establishing remediation priorities and recommendations.

Project Objectives

The overall objective of this project is to understand, at a high level, the breadth and cost of legacy system remediation and modernization across State of Texas agencies. The objective of the report is to provide state leadership with data on whether to replace or update aging systems. Meeting these objectives included

- Determining the size, maintenance cost, and risk of legacy systems within the state based on data collected
- Applying a standard, adaptable, methodology to standardize and prioritize systems into groups based on functional similarities, then

increasing data quality with industry research and state agencies' perspectives

- Determining feasibility of remediation for groups of legacy systems and for high-value, individual legacy systems by using industry best practices
- Objectively identifying modernization opportunities and associated estimated costs

Analysis Approach

The project required a great deal of analysis by the project team to summarize the wealth of information gathered during the inventory phase. This analysis was essential in forming meaningful recommendations.

- For a project of this scope, portfolio analysis can be as broad or deep as desired—the degree to which it can be either is a function of the quality and availability of data and the time available to conduct the analysis.
- This report provides a broad analysis of state agencies' application portfolios (i.e., their collections of IT systems, including related hardware and software), and provides an evaluation of technical condition, business value, and cost of these state assets.
- With the framework and tools provided by this project, DIR and state agencies will be able to continue the analysis to explore areas of interest and gain deeper insights.
- The recommendations in this report reflect the broad analyses undertaken and identify steps to continue progress in updating these IT systems, a process referred to as legacy modernization.

Assessment Results

The study identified more than 13,000 physical and virtual server (hardware) instances and 100,000 software product instances that support the state's systems. In turn, these systems support more than 4,130 business applications.

Business application names are the high-level labels used by the agency business and IT organizations to easily reference a group of functions provided by the systems.

The Legacy Systems Study found that over half of the 4,130 business applications contained in agency application portfolios are considered legacy. This designation is based on whether a business application relies upon hardware and software technology that is no longer supported under standard vendor support. In some cases, only a small portion of the underlying technology is legacy, but in the majority of cases, most of the technology is outdated. Legacy business applications are more difficult and costly to support, are less resilient, and are likely to carry a higher degree of security risk.

The legacy portion of the statewide application portfolio includes business applications of all functional categories from across almost all agencies. It encompasses large systems of record, including many mission-critical business applications, as well as smaller systems. The legacy applications cannot simply be dismissed because agencies indicate that core, mission-related, functions rely on these systems. This presents a conundrum: these business applications are valuable, yet their technical underpinnings need to be replaced or updated (remediated) to support agencies' IT needs.

There is a range of feasible remediation options available for such legacy business applications, from limited software and hardware upgrades to full replacement, depending on the characteristics of the application. The Legacy Systems Study presents various options and maps them to different applications. When considering these options, it is beneficial to approach modernization at a holistic or portfolio level so that system interdependencies are considered.

The state would also benefit from reducing the number of software products and optimizing its technology landscape to reduce costs and risks associated with outdated or unsupported applications. For instance, there are many applications across the state that provide similar functionality. Examples include applications related to functional areas such as licensing services, or technology areas such as reporting. In total, agencies use over 4,200 unique software products, installed in over 100,000 instances, with 61% of these instances considered legacy. A reduction in the variance of software products would reduce the size and complexity of the future application landscape after remediation.

There are many reasons that the technology that supports business applications becomes legacy. The demand for IT always outpaces supply, and agencies must balance investments in systems that support daily activities and provide immediate business value with technology maintenance, which provides less tangible benefits in the short term. As the state continues to attract more citizens and experience significant business growth, the demand for state-provided services increases. Because agencies are often unable to add staff to meet the growing demand for services, there becomes an increased dependency upon automation to meet that need. Over time, technical debt accumulates and becomes harder to reconcile.

The current annual ongoing cost of the state's legacy portfolio, based on support effort and software license fees, is over \$300 million. Based on a formula for a high-level remediation cost estimate at a portfolio level, the one-time cost to remediate the technical debt within legacy business applications on an agency-by-agency basis will likely exceed \$450 million when not taking into account opportunities to share services. The

cost and complexity of individual legacy business applications is substantial, and consolidation would avoid redundant remediation effort.

Recommendations

Recommendation 1. Agencies should develop a prioritized impact analysis and mitigation plan of identified legacy system security risks.

If agencies understand and prioritize the impact of replacing and/or upgrading aging infrastructure, business decisions can be made more easily. The identified risks are primarily a result of running older software and hardware that can no longer be updated with security fixes, nor support modern security implementations. These mitigations would not imply a full legacy modernization, but would target security risk mitigation. Such an analysis can result in a strategy that allows for targeted upgrades that could be implemented in phases based on available resources.

Recommendation 2. Amend [Texas Government Code \(TGC\), Chapter 2054](#) to authorize DIR to develop a legacy modernization strategy and to collaborate with agencies to use comprehensive strategies, developed as part of the Legacy Systems Study and identified in this report, as guidance in their legacy modernization efforts.

This recommendation would allow the state to take the next step toward developing a modernization strategy, both at the state level and in concert with agencies at the agency level. The Legacy Systems Study indicates a number of areas of prioritization based on the business value, technical quality, and cost of business applications. The Legacy Systems Study identifies remediation options, including a preliminary mapping to business applications. However, this study is not a comprehensive strategy toward legacy modernization.

Recommendation 3. Amend TGC 2054 to authorize DIR to build upon the legacy modernization strategy by

- *Establishing a statewide application development framework*—A framework is a recommended approach that provides direction and structure for agencies to follow. Currently, there is no statewide framework for software application development.
- *Facilitating standardization and collaboration*—A modernization strategy is a roadmap for pursuing opportunities for technology standardization, reducing the variety of technologies within the statewide portfolio, and seeking opportunities to consolidate business applications into fewer solutions, both within and among agencies.
- *Achieving economies of scale by leveraging agency investments*—As part of the Legacy Systems Study, DIR sponsored a workshop with many agencies where representatives indicated an interest in common solutions and technologies among agencies. This shared approach would yield long-term cost reduction and operational benefits.

Recommendation 4. As part of a legacy modernization strategy leveraging common solutions, agencies should prioritize commercial off-the-shelf (COTS) solutions over custom-developed replacement solutions.

Standardization and consolidation should include an emphasis on shared solutions including those delivered as services through the cloud (i.e., via the Internet instead of through an organization's own technology infrastructure) where possible, reducing the number of custom-developed business applications. The analysis of software components indicates that there is a high degree of custom-developed solutions, even in application categories where there are

off-the-shelf solutions available. While agencies have diverse business needs, custom applications that create a solution from the ground up may not be needed.

Recommendation 5. Amend TGC 2054 to authorize DIR to implement a shared (multi-tenant) reporting services and business analytics pilot to determine the viability of a statewide solution. Such a capability provides administrative services and tools to manage the IT function, including software tools that manage data reporting and business analytics (data analysis that reveals trends and enables predictions for optimization of business performance). This would allow agencies to consolidate disparate software and hardware onto a consolidated platform. Such a platform, offered as a service, would accelerate remediation of legacy reporting applications and provide higher level business intelligence capabilities to agencies.

Recommendation 6. Amend TGC 2054 to authorize DIR to establish a voluntary pilot program that provides statewide application portfolio management (APM) practices and toolsets for agencies to implement any recommendations following the Legacy Systems Study. An APM would help agencies approach their IT management from a global perspective, improve statewide application management, and provide opportunities for efficiencies. In the current environment, there is limited active portfolio management to guide decision-making for IT investment, or to balance business needs that drive functionality with the requirements of maintaining the technology landscape and sustaining business applications. DIR is well positioned to assist with the statewide perspective of portfolio management: it has insight into agency portfolios and direction and can provide advice on

pragmatic application consolidation that yields long-term benefits.

Note that all recommendations are based on and related to only the agencies included in the study.

Texas attracts nearly half a million new citizens annually and is prospering due to a positive business climate, desirable quality of life, favorable cost of living, and an independent spirit. These characteristics challenge state government to ensure that Texas retains its national leadership position and continues to provide statewide services that meet the needs of its citizenry. Agencies depend upon their IT systems to deliver state services and must be in a position to grow these systems in an agile and fiscally responsible manner.

This study, and the resulting recommendations, present a unique opportunity to fully understand the health of these systems and the actions necessary to operate an efficient and cost-effective state government.

High-Level Findings

Architecture Analysis

The state's application portfolio comprises more than 4,130 business applications supported by the state's systems. Of these, approximately 58% are listed as legacy because they contain legacy components. In most cases, these legacy business applications are supported by both legacy software and hardware:

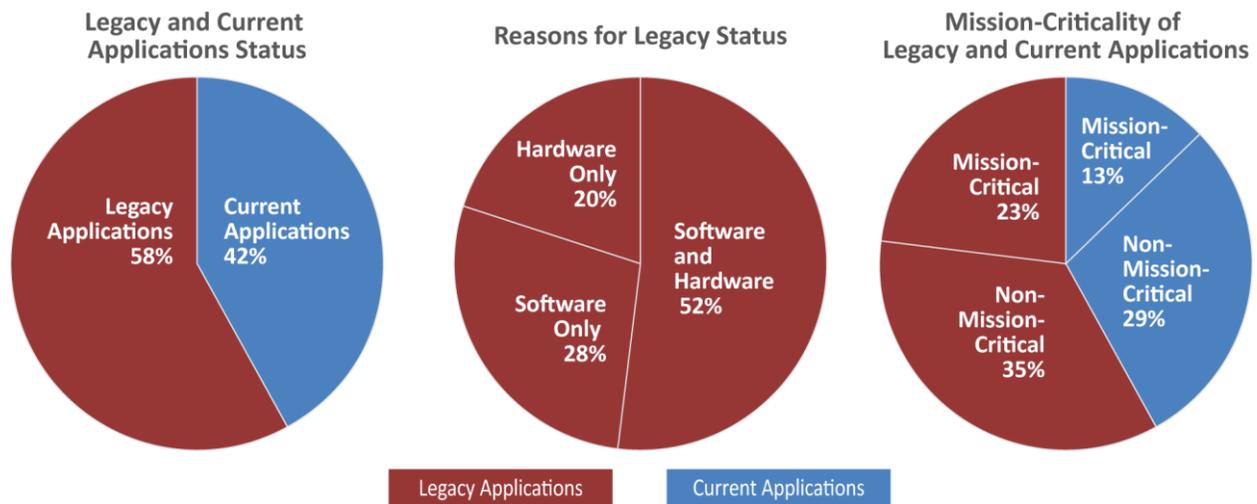
- 52% of the legacy applications use both outdated hardware and software
- 20% of the legacy applications use outdated hardware
- 28% of the legacy applications use outdated software

Mission-Critical Applications

Approximately 36% of the entire state application portfolio is deemed mission critical by agencies, while 64% is not mission critical.

Almost two-thirds of the mission-critical applications have legacy components, while the remaining third is current. Just over half of non-mission-critical applications are considered legacy, while the remaining are current.

Overall, the mission-critical applications have a higher legacy ratio than non-mission critical applications.



The remainder of this section presents the results of high-level analysis of the state's business applications, which have been grouped according to 33 functional categories. DIR asked agencies to categorize their business applications by function, realizing that a single agency-identified business application could provide functionality in multiple categories. Agencies provided up to three prioritized categories per business application.

Note: The functional categories are identified by short names or keywords in the charts and text below. Each functional category is more fully defined in the [Appendix](#) (page 15).

Hardware and Software Components by Primary Functional Category

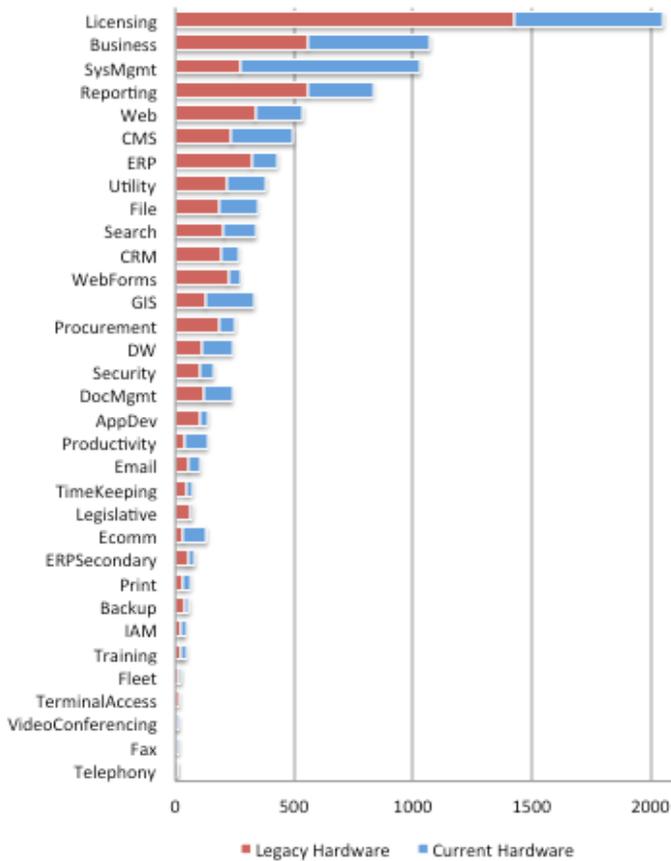
Business applications are made up of hardware and software components. The largest numbers of these components are related to the following functional categories:

- Licensing/Permitting/Monitoring/Enforcement
- Business Automation
- Systems Management

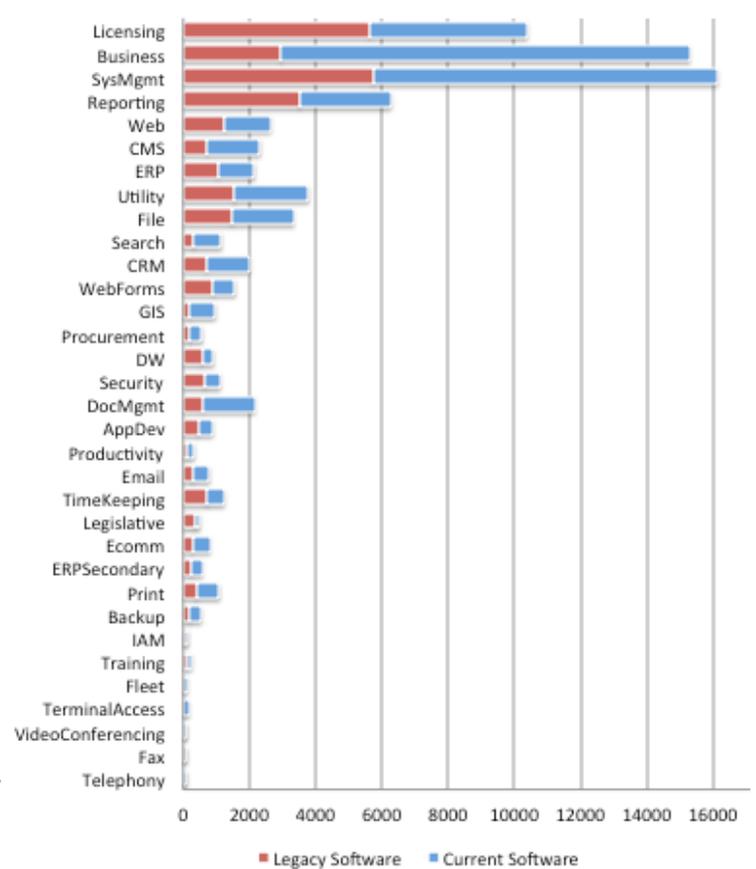
- Reporting Systems
- Web Systems
- Content Management Systems
- Enterprise Resource Planning

The legacy ratio between the hardware components or software products is not significantly different among the categories.

Hardware Components by Primary Application Category



Software Components by Primary Application Category



Legacy Remediation Cost Estimate

A high-level remediation cost estimate for the entire legacy application portfolio across all functional application categories is approximately \$450M. The majority of remediation cost is within the functional categories identified as focus areas:

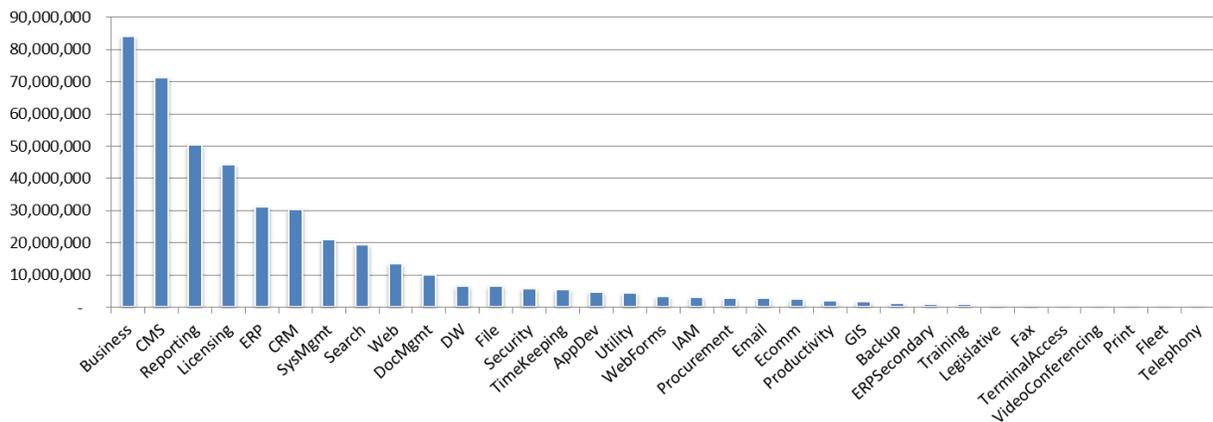
- Business Automation
- Content Management Services
- Reporting
- Licensing/Permitting/Monitoring/Enforcement

- Enterprise Resource Planning
- Customer Relationship Management
- Systems Management
- Search

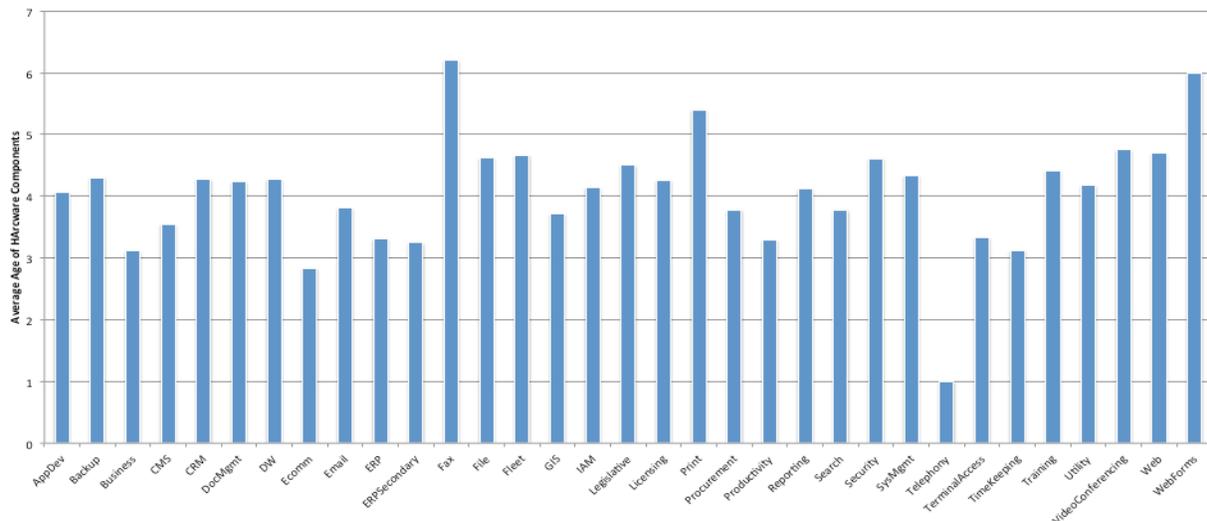
Average Age of Hardware Components

The average age of existing hardware components varies across functional categories, though not significantly. These averages would be expected to be lower when subject to a more uniform refresh cycle (the industry standard is to refresh hardware every three to five years).

High-Level Estimate of Legacy Remediation Cost by Business Application Category



Average Age of Hardware Components



Recommendation 1

Determine the Impact of Identified Security Risks and Prioritize Mitigation

Agencies should develop a prioritized impact analysis and mitigation plan of identified legacy systems' security risks. Agencies reported a number of applications that have unresolved security risks introduced by relying on legacy systems. These security risks include the inability to implement updates on older software, as well as implementation configurations that diminish security capabilities. A number of the involved applications provide significant business value, and some are mission critical. These applications cannot wait for legacy remediation—the identified security vulnerabilities must be addressed as soon as possible.

Even if applications are “behind the firewall” (guarded by network protections), it is imperative to have all known security risks mitigated with urgency. This likely requires operating system or software product upgrades, or both. At minimum, the impact is time and effort for implementation and testing. In some cases, de-

pendencies between software products (and potentially between software and hardware components) require broader updates. A key step is to identify these dependencies and develop a plan to resolve the security risks with consideration for the amount of change and relative impact.

An impact analysis and remediation of these risks would:

- Determine the potential impact of the security risks identified by agencies
- Develop the most expedient and least disruptive approach to mitigate the risks
- Implement mitigation initiatives

Prioritizing the impact analysis and risk mitigation has the following benefits:

- Reduces the potential vulnerability of agency applications and data
- After mitigating the risk with minimal solutions, reprioritizes further remediation based on the overall legacy remediation strategy

Recommendation 2

Develop a Legacy Modernization Roadmap Strategy

Amend TGC 2054 to authorize DIR to develop a legacy modernization strategy and collaborate with agencies to use the comprehensive strategies as guidance in their legacy modernization efforts.

Many of the remediation options are complex. Large-scale modernization efforts carry a significant amount of risk that can be reduced by developing a structural, yet pragmatic, approach toward implementation.

This study assessed the statewide application and technology portfolio, resulting in a number of findings. Key among the findings is that the legacy issue is widespread, both among agencies and among application categories. It will take a significant amount of effort and investment to remediate the portfolio and reduce the risks associated with legacy systems, including security vulnerabilities and lack of timely support. A comprehensive roadmap at the statewide level to guide agency initiatives would drive the effort to

remediate the legacy portfolio at both state and agency levels.

A legacy modernization strategy would:

- Identify specific initiatives to remediate legacy applications
- Prioritize initiatives across agencies based on business value and risk reduction
- Develop a mechanism to track the effectiveness of these initiatives

- Establish milestones, metrics, and validation of outcomes

Implementing a legacy modernization strategy would provide the following benefits:

- Maximizes the technology investment in terms of business value
- Ensures the proper prioritization of initiatives
- Ensures the use of effective and common approaches across agencies

Recommendation 3

Leverage DIR to Establish a Statewide Application Development Framework, Standardization, and Consolidation

Amend TGC 2054 to authorize DIR to establish a statewide application development framework and to facilitate standardization and collaboration, achieve economies of scale, and leverage agency investments.

Recommend that DIR create a function to provide strategic information technology advice and guidance to state agencies through direct engagement to promote enterprise architecture standards, collaborative communities, and awareness of technical initiatives.

Statewide Application Development Framework

The current statewide application portfolio is a collection of agency portfolios: there is no particularly strong, coordinated driver to seek economies of scale or leverage agencies' investments at other agencies. There are some examples of such collaboration at the agency level, but it is not approached systemically. Objectives expressed in other recommendations, including standardization and implementing a preference for commercial off-the-shelf (COTS) solutions, depend on a common partner to facilitate collab-

oration among agencies and to present a cohesive approach to the Legislature. DIR is uniquely positioned to perform this role.

Leveraging DIR to establish a statewide application development framework would:

- Facilitate consistent, structured cross-agency engagements such as round-table discussions and an application-based coordinating council
- Build a community of interest
- Seek ways to leverage common solutions
- Enable DIR to actively pursue opportunities to drive value from agency technology investments

Implementing a statewide application development framework would have the following benefits:

- Actively implements a framework that will be used to create a statewide legacy modernization program
- Facilitates collaboration and alignment of application development practices among agencies
- Enables the recommendations to improve standardization and increasing the use of COTS solutions

The need to modernize legacy systems is a challenge as well as an opportunity. Rather than implementing modernization as a technology-centric program, DIR can help to approach modernization from an application perspective. As technology infrastructure becomes more commoditized over time, the majority of cost, as well as business benefits, are a result of organizations' application strategies. At this stage, most agencies do not have a strong discipline in this area, and legacy modernization provides the impetus for a statewide perspective.

Standardization and Consolidation

Amend TGC 2054 to authorize DIR investigate the opportunity to standardize technologies for common agency solution areas. This could reduce redundancy, provide better insight into data, and leverage skills across agencies. By focusing less on the technology and more on the implementation of the technology, the state could develop best practices for functional areas among agencies. The first step of the investigation would be to develop a model to quantify the potential benefits and metrics to measure success.

Agencies use a number of similar applications across similar business functions, but these applications are often implemented with different technology products, which overlap in functionality. Instead of approaching these applications as unique solutions, common approaches and technologies can be leveraged by multiple agencies. A number of applications in different categories, including Customer Relationship Management (CRM), Enterprise Resource Planning (ERP), Licensing / Permitting / Monitoring / Enforcement (Licensing), and Search, are currently in legacy status and need to be remediated. Instead of addressing these applications individu-

ally, DIR should facilitate working groups and collaboration with agencies to perform application-level analysis to determine commonalities and pursue common solutions.

Standardization and increased shared solutions would:

- Replace distributed technologies with common solutions
- Introduce best practices-based approaches across agencies
- Potentially replace distributed hardware with centralized and shared hardware
- Establish common test environments for agencies to quickly ramp-up projects

Standardization and increased shared solutions have the following benefits:

- Improves the time-to-market to deploy solutions through shared knowledge and experience
- Encourages collaboration among agencies across the state
- Develops an understanding of common data and encourages sharing data among different agencies in the same business areas
- Allows for sharing of expertise and skills

Recommendation 4

Seek Commercial Off-the-Shelf Solutions over Custom-Developed Solutions

As part of a legacy modernization strategy, the state should seek to prioritize the implementation of COTS-based solutions wherever it makes practical sense. COTS solutions include cloud-based implementations, particularly Software-as-a-Service (SaaS, or sharing applications) and Platform-as-a-Service (PaaS, or sharing the technology to build applications) solutions.

Of the many business applications in use across agencies, there is an emphasis on custom-developed solutions. Although the use of a COTS product as the main solution is not explicitly tracked, the number of COTS products among the most commonly used software in application categories is limited. The number of different software products in use is large, and there are many specific solutions. In many cases where agencies have embarked upon legacy modernization programs, they have adopted a preference for COTS-based solutions over custom-developed replacement, especially for slowly evolving systems that provide transactional functionality.

A preference for COTS-based solutions over custom-developed solutions would:

- Replace existing legacy custom applications with COTS-based solutions
- Standardize COTS products across agencies in similar functional areas
- Leverage industry best practices, embedded in COTS solutions, to support future state business processes across agencies

Implementing a higher degree of COTS solutions would have the following benefits:

- Reduce the complexity of the statewide application portfolio
- Reduce the number of technologies
- Reduce the dependency on specialized resources only found within a small number of agencies
- Encourage collaboration among agencies across the state
- Encourage data sharing data between different agencies in the same business areas

Recommendation 5

Consolidate Reporting and Analytics into Consolidated Business Intelligence Services

Amend TGC 2054 to authorize DIR to implement shared (multi-tenant) reporting services and business analytics capabilities. This could reduce redundancy, provide better insight into data, and standardize skills across agencies. By reducing agencies' need to focus on distributed reporting technology, they would be better equipped to focus on establishing and tracking key performance indicators.

Many agencies deploy reporting and data warehousing capability, either as a focused application category or as part of business automation, Customer Resource Management (CRM), and other types of applications. Agencies use a variety of reporting tools, and a significant portion are considered legacy. In some cases, reporting is performed against applications' operational databases, but in other cases (and following best practices), agencies establish separate reporting databases.

There is an opportunity to consolidate reporting capability into a shared service, which would provide agencies with the tools and technologies needed to perform reporting and/or data warehousing, especially in cases where agencies utilize separate reporting databases.

This shared service would:

- Provide agencies with consolidated, up-to-date, and maintained tooling
- Replace distributed reporting hardware with centralized and shared hardware
- Provide standardized and powerful data cleansing and aggregation tools

A shared reporting service has the following benefits:

- Reduces the proliferation of hardware and software related to common reporting functions
- Encourages sharing of data and establishment of master data across the state
- Reduces the risk of reporting applications becoming legacy in the future
- Allows for sharing of expertise and skills

Recommendation 6

Implement Application Portfolio Management Practices

Amend TGC 2054 to authorize DIR to establish a voluntary pilot program that provides statewide application portfolio management (APM) practices and toolsets supporting agency implementation of any recommendations following the Legacy Systems Study. This could provide consistency in the data, enabling reliable review and continuous improvement across the state enterprise. It also allows agencies opportunity to collaborate more effectively on similar business requirements. It may be one of the first steps to deploying statewide Master Data Management, Application Programming Interface (API) service registry, and Enterprise Service Bus solutions.

APM's goal is to describe the inventory of applications and the resources (e.g., money, staff time, infrastructure) required to provide operational support of those applications over their lifetime. APM is closely related to governance and how an agency ensures that applications are aligned with agency business needs, enterprise architecture (alignment of people, processes, technology), and tracking of effective metrics to

measure the cost/value proposition of applications relative to each other within an agency (or state) portfolio. APM should guide the investment decisions for an application's lifecycle, particularly balancing between adding features, maintaining infrastructure currency, and modernizing the platform. Effective implementation of APM is an indicator of an organization's information technology services maturity and its ability to respond to business requirements.

Application portfolio management is used to:

- Identify application investment requirements
- Identify and tracks costs
- Establish application lifecycle expectations (at least estimations)
- Measure, report, and adjust values and expectations
- Track against original expectations
- Track large changes to requirements over the life of the application

Application portfolio management provides the following benefits:

- Ensures ease of ongoing visibility to applications' relative business value
- Guides the business and information technology organizations in prioritization
- Enables rationalization across business, agency, and enterprise where possible

Appendix

Functional Category Definitions

Application Development (AppDev)

Components related to the development and maintenance of applications.

Backup/DR Systems (Backup)

Components related to disaster recovery, data backup, and business continuity.

Business Automation (Business)

Manages the integration of systems via messaging, transformation of data, and scheduling of transactions.

Content Management Systems (CMS)

Includes document management (born-digital documents, not scanned), electronic records management, web-content management, knowledge management, search and retrieval, content categorization (taxonomy), digital preservation, and email archiving.

Customer Relationship Management (CRM)

Includes service and support systems designed to increase the productivity and efficiency of support staff who are required to support constituents and service requestors. This is a front-office customer service and support category.

Data Warehousing (DW)

Includes reporting, analytics, and business intelligence in order to support data analysis and decision-making tasks.

Desktop Productivity (Productivity)

Equipment, applications, or services used to aid employees with their productivity.

Document Management Systems (DocMgmt)

Includes different aspects of converting paper documents to electronic form, such as imaging, scanning, indexing, electronic forms, back-file conversion, workflow, optical character recognition, computer output to laser disk, and computer output to microfiche.

E-Commerce (Ecomm)

The buying and selling of products or services conducted over electronic systems such as the Internet and other computer networks. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

Enterprise Resource Planning (ERP)

Includes the administration of an organization's financial and human resources back-office systems that include general ledger, accounts payable, accounts receivable, budgeting, inventory, asset management, billing, payroll, projects, grants, payroll, and time and labor.

ERP Secondary (ERP Secondary)

Ancillary accounting applications that gather and feed data to a primary accounting system (cash management, employee time, and leave tracking).

Fax Services Systems (Fax)

Fax Services Systems allows for the production, retrieval, storage, and printing of faxes to and from the agency.

File Services (File)

Standard file and data storage used for daily business operations.

Fleet Management (Fleet)

The management of a company's transportation fleet. Fleet management includes commercial motor vehicles such as cars, ships, vans, trucks, and rail cars. Fleet management can include a range of functions, such as vehicle financing, vehicle maintenance, vehicle telematics (tracking and diagnostics), driver management, speed management, fuel management, and health and safety management.

Geographic Information Systems (GIS)

Includes the capturing, storing, updating, manipulating, analyzing, displaying, and/or online publishing of geographically referenced information.

Identity Management (IAM)

Includes components providing authentication and authorization, such as single sign-on, digital certificates, etc.

Legislative Tracking (Legislative)

Data repository used to track new and old legislation that may apply to an agency. Allows the agency to plan for, respond to, and manage change resulting from the legislation.

Licensing/Permitting/Monitoring/Enforcement (Licensing)

Includes systems that support licensing and/or permitting functions of the agency, and/or related activities such as compliance monitoring and enforcement.

Messaging/Email Systems (Email)

Components supporting messaging systems, including email, instant messaging, and their security.

Online Web Forms (WebForms)

Web-based online forms for data entry to a back-end system.

Print Services (Print)

Devices providing standard print services function for daily business operations.

Procurement (Procurement)

The acquisition of goods, services, or works from an outside external source.

Reporting Systems (Reporting)

Toolsets and applications that have the proper drivers to attach to databases and provide reporting for the various agency needs.

Search System (Search)

Tool for searching back-end systems.

Security Systems (Security)

Includes network and client-based firewall and virtual private network (VPN) deployments; intrusion prevention or detection systems (IPS/IDS); server-based access controls (e.g., biometrics, smart cards/other one-time password tokens); encryption (for data in transit, files, public key infrastructure); IT security design reviews; vulnerability scanning, assessment and testing; malware blocking tools (e.g., application-level attack blocking, virus, spyware, adware, and spam management); automated patch management and security policy compliance tools; physical security for IT assets; and the implementation of forensics, risk, or security assessment tools.

Systems Management (SysMgmt)

Systems management addresses technologies used to manage and monitor the network, servers, applications, and other elements of the IT infrastructure, which can include systems management and monitoring, performance management, change and release management, and software distribution.

Telephony Systems (Telephony)

Includes interactive voice response (IVR), voice over Internet protocol (VoIP), hosting and management of call centers or contact centers.

Terminal Access Systems (Terminal Access)

Services that allow connectivity to external systems with which the agency must share data. For example, connectivity to applications from the Texas Comptroller of Public Accounts that make up the agency primary accounting system. Also includes remote access components such as Citrix, XenApp, Radius, etc.

Timekeeping Systems (Timekeeping)

Agency system used to document time spent by staff on projects.

Training (Training)

Provide interface for presenting training materials and tracking completion.

Utility Systems (Utility)

These may be hosted domain name system (DNS) services, dynamic host configuration protocol (DHCP) services, virtualization services, system monitoring, logical security services, terminal emulation services, remote access services, or others that are applied to one or more other servers.

Videoconferencing/Web Broadcasting (VideoConferencing)

Includes two-way analog or IP-based videoconferencing, as well as IP-based video broadcasting (one-way, one-to-many, and replay).

Web Systems (Web)

Public facing or internal agency websites and their supporting components (security, monitoring, etc.); includes FTP sites.