Identity and Access Management Feasibility Analysis

November 30, 2016

Texas Department of Information Resources

Contents

1. Background and Summary

As personal information and individual state user profiles continue to expand, organizations must ensure that they avoid redundancies and increase the security profile of the state by implementing new identification and access requirements for certain information. SB 1878 (84R) required DIR to perform an analysis on the implementation of new identification and access requirements for accessing state information and to develop a strategy by which DIR can negotiate for bulk purchases across agencies.

This analysis was to determine available options for identity and access management (IAM). IAM is an organization's use of security and business governance that ensures that individuals are only accessing the right resources when necessary and for legitimate purposes.

IAM is not a single technology, but rather a system of capabilities that can enhance information security, provide enforcement for policies and standards, reduce administrative overhead and reduce the likelihood of data exposures and leakage through vigilant management.

DIR contracted with Gartner, an international information technology research and advisory company, to conduct an IAM Study to facilitate information discovery and incorporate input from agencies and Institutions of Higher Education (IHE). Information was gathered from a web survey sent to all 183 state agencies and IHEs, interviews with the State Information Security Advisory Committee (SISAC) members and data gathered from the 57 Gartner Security Maturity Assessments conducted over the previous four years.

While several of the larger agencies and Institutions of Higher Education have implemented solutions of their own, the majority of the agencies have not. The data gathered indicates a low level of maturity in the areas of identity and access management for a majority of state agencies.

Although there is a low level of maturity, there are numerous options available for agencies interested in IAM as shown below. Particularly, three main options offering varied levels of IAM support and cost are listed and include annual costs for up to 10 years.

The IAM Study identified several areas that could be improved by implementing an IAM solution, including efficiency of IT resources and information security. The complete IAM report is available upon request.

1.1. Efficiency: Reduced Administrative Overhead

Keeping the required flow of business data moving while simultaneously managing its access has always required administrative attention. The business information technology (IT) environment evolves daily and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), bring-your-own-identity (BYOI), cloud computing, mobile apps and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges.

As employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. Automated workflow and provisioning capabilities can provide a return on investment (ROI) for medium to large organizations while freeing administrative resources. Manual provisioning is labor intensive and usually involves individuals from across disciplines and departments to ensure that all needed

entitlements have been provided. As an example, access to a single application may require the involvement of the help desk, a server administrator, an application developer, a database administrator, and the application owner/manager for approval.

1.1.1. Maintaining Systematic Enforcement and Ease of System Administration

Most organizations already have policies designed to ensure proper oversight of system access is maintained. Many of these policies are driven by legislative or compliance requirements. However, in some cases, these policies have not been fully institutionalized or consistently enforced.

Automated policy enforcement is required for comprehensive access risk management to ensure that risk is properly monitored, managed, and mitigated. Furthermore, delegated policy enforcement allows a master policy to be established and enforced, while also allowing individual business or organizational units to establish their own policy based on unique needs, all within the framework of the master policy.

1.2. Information Security

A lack of effective identity and access management poses significant risks to an organization's overall security. Ensuring the correct personnel have appropriate access to systems and information is a key tenant of information security and is the purpose and foundation for IAM technologies.

1.2.1. Preventing Inappropriate Access

The foundation of any access management initiative should be adherence to the principle of least privileged access: legitimate users should have no more access than the minimum required to perform their jobs.

Inappropriate access results in an increased risk of unauthorized access to sensitive applications and data, as well as reduced confidence in the security posture of the organization and the ability of the infrastructure, systems, and applications to provide appropriate level of data protection commensurate with established enterprise security objectives. IAM related technologies can mitigate inappropriate access in several ways.

1.2.2. Limiting Data Exposures or Leakage

Information protection may not be applied commensurate with the risk presented by the use of specific information, potentially resulting in data exposure, leakage or loss of data integrity. Data exposure, intentional or not, can be the result of theft, inadvertent exposure, neglect, abuse, or unsecure business processes.

Using good, hygienic data and system access processes can help offset the risks associated with system breaches and includes practices such as using privileged access management, separate administrative accounts for managing systems, account review and approval and removal of unused, and terminated user accounts.

2. IAM Technology Components

IAM can be comprised of multiple components, some of which are detailed below.

2.1. Directory Services

Directory services are the foundation for all IAM initiatives since it serves as either a source of data to be stored in the directory or consumes data stored in the directory. All user authentication uses the directory as the authoritative source of a user's credentials. The directory also stores group memberships and user attributes such as name, address, phone, organizational position, relationship, along with other pertinent information.

Performance of the directory service has a direct effect on the performance of all applications or IAM-related components that interact with it. Outages in a directory service can bring all connected services to an immediate standstill. Critical state functions such as law enforcement, emergency response or healthcare require highly available directory services in order to maintain acceptable public service levels.

2.2. Globally Unique User Identifier (GUID)

The objective for a globally unique user identifier (GUID) is to provide an authoritative identifier that would uniquely identify a state employee. A GUID would simplify cross-agency management and assist with reconciliation when two-similarly named individuals are encountered by different agencies. For identity and access management, the authoritative source for GUID's is usually Human Resources since their data is maintained regularly and regarded as accurate.

Any identity information linked to the GUID contained in the system (e.g., first name, last name, address, department or email) can be accessed and utilized by other systems in leveraging user identities.

2.3. Encryption/Public Key Infrastructure Certificate Services

Public key infrastructure is an encryption and authentication approach where a pair of keys are used to encrypt, decrypt and verify the identities of users and networks when exchanging data.

2.4. Multi-Factor Authentication (MFA)

The authentication process is one of the most critical functions for protecting access to data and network systems and involves a user providing a claimed digital identity, usually in the form of a user ID. Single-factor authentication involves something that the user knows, such as a password. Multi-factor authentication involves an additional corroborating piece of information—something the user possesses--that can be used to validate the user's authenticity.

2.5. Privileged Access Management

Generally, privileged access is access to systems, resources and processes above that of a standard user and can include full control over key information technology resources. If

compromised, these privileged accounts can be used to wreak havoc on critical systems and infrastructure.

Privileged access management (PAM) solutions have been developed to strictly control how administrators or other privileged users access these privileged accounts.

2.6. Identity Proofing

Identity Proofing (also known as Identity Verification) verifies people's identities prior to the agency issuing an account and credential. The objective is to provide a mechanism to establish the identity of a user to the level of assurance required by the level of access being granted.

2.7. Automated Provisioning and Workflow

Automated provisioning is the ability to manage access to IT resources by using pre-defined procedures based on business logic that are carried out electronically through workflows without requiring human intervention. User accounts are automatically created, modified or disabled based on inputs from authoritative data sources.

2.8. Web Access Management (WAM)

Web access management systems enable enterprises to provide common authentication and authorization services for web based resources (whether internal or external facing). With these systems in place, the objective is to provide access with a consistent logon credential to inter-agency applications (CAPPS, ERS, etc.)

2.9. Federated Identity Services

A federated identity service is the linking of a person's electronic identity and identifying information, stored across multiple systems allowing the user to obtain access to the networks of all systems in the trusted group through the use of a single sign on.

2.10. Components Summary

IAM technologies can be used to enhance information security by providing technological enforcement of policies and processes as part of web access management, federation and automated provisioning. In addition, security can be further improved through the use of encryption technologies such as public key infrastructure, as well as controlling system and user access through the use of multi-factor authentication and privileged account management technologies.

3. Potential Cost Savings and Cost Avoidance

Implementation of IAM solutions not only provide additional security through automated enforcement and processing, but the automation of provisioning and access management can also present a ROI. For the purposes of this study, calculating these potential cost savings requires a level of detail not gathered for each individual agency. However, a high-level approach for the types of savings available are outlined in the sections below.

3.1. Cost Savings from Improved Efficiency and Increased Productivity

True cost savings result mainly from the implementation of automated provisioning workflows and self-service tools that reduce headcounts required to manually administer access to an agency's information systems.

3.2. Additional Potential Cost Savings and Intangible Impacts

Additional tangible cost savings exist for the state depending on each agency's business process costs and staffing models. With agency specific insights, calculating the benefits of improved workflow, business processes and business improvements can be explored further.

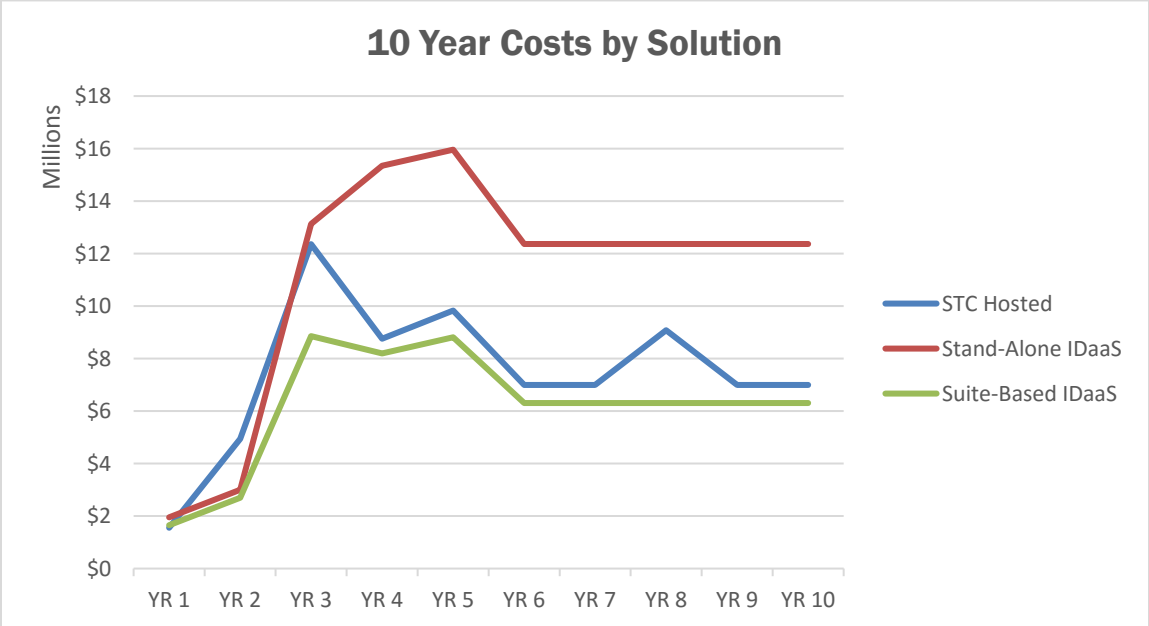
3.3. Cost Avoidance: Compliance and Protection

Providing secure and appropriate access to the State's information is the purpose of IAM technologies. The cost of data exposure or breaches has been increasing steadily with additional penalties associated with non-compliance.

4. Purchase of statewide IAM solution

The possible IAM delivery models were evaluated to determine the benefits of a solution that is hosted and maintained in the state's central data center by the Statewide Technology Center (STC) contractor versus procurement of a demand-based, user-priced Identity as a Service (IDaaS) offering.

Figure 1 10 Year Costs by Solution



1. STC Hosted Total 10 year cost: $ 74,499,000
2. Stand-Alone IDaaS Total 10 year cost: $111,210,000
3. Suite-Based IDaaS Total 10 year cost: $ 61,740,000

4.1. Infrastructure cost for STC implementation

The STC Hosted option has several advantages, including the existence of a service model and contract in place. The licensing for the platforms is already in place as well, saving additional implementation costs. However, disadvantages including skillset availability and a longer start-up time for system implementation prior to the services being available to the first user must also be considered. Additionally, the architecture costs are the same for one user or one-million users, meaning a large portion of the expenditure is up front.

4.2. SaaS Solution

The Software as a Service (SaaS) option provides the greatest amount of flexibility for the State, both in ability to stage a roll-out for slower agency-adoption and highest discounts available for the suite-based pricing.

4.2.1 Additional SaaS Considerations

Pricing of a SaaS solution is determined by scope (bundled services vs a la carte), volume and length of contracts. Bundled services are offered by multiple vendors at prices far below the individual component costs of the services if provided separately. A bundled solution allows the state to evaluate the types of service volume discounts that are available by purchasing an integrated solution from a single vendor. A la carte pricing, for a non-integrated solution with potentially different vendors supplying each service, would not be cost effective for a statewide implementation. Refer to Figure 1 for details.

4.3. Suggested Solution

The IAM Study recommends a time-phased deployment approach for the adoption of an integrated solution referred to as IDaaS, using a cloud-based service provider, with the initial offering limited to 102 agencies. To ensure implementation success, the creation of a Global Unique User Identifier (GUID) provides a unique identifier for each user. Not only is this a best practice, but it provides additional security of user-specific information.

The IAM Study also resulted in several governance recommendations, beginning with the establishment of a statewide IAM Governance body to guide the implementation of the project. Second, identity proofing processes are recommended to align the identity vetting activities with access enforcement based on the level of assurance required. Similarly, the third governance recommendation, system proofing, aligns with assurance activities such as the creation of DIR's Statewide Data Coordinator role.

Finally, the creation of a Center of Excellence (COE) will assist agencies with onboarding, including IAM-specific processes, best practices, and critical aspects of data standards and other considerations to ease transition into the centrally-provided services.

4.3.1. Time-Phased Implementation

A four-phased deployment approach would deliver a modular, fully encompassing IAM infrastructure. The phasing is detailed below:

- Phase One: Immediate – Planning and Design Activities. The immediate phase encompasses planning, design, data quality, governance, process changes and initiation of potential legislation. This phase includes creating an IAM Center of Excellence to assist the agencies with onboarding during their initial implementation, as well as establishing an IAM Governance Committee to oversee these efforts.
- Phase Two: Near-Term – Directory Services, Multi-factor Authentication Deployment. This phase focuses on the implementation of a single, centralized statewide directory including creation of a Globally Unique User Identifier (GUID) and will be leveraged by all other services. At this point, the state would start deploying multi-factor authentication.
- Phase Three: Mid-Term – Privileged Access Management and Automated Provisioning. This phase includes implementing privileged account management (PAM) for service and application accounts. With identity proofing in place, the automated provisioning for onboarding can begin.
- Phase Four: Long-Term/Future Considerations – Web Access Management (WAM) and cloud-based Federation. This phase focuses on enhancing the access control infrastructure with web application controls and provides central, standard, secure application authentication. This phase also includes advanced certificate authority/public key infrastructure (PKI) capabilities including encryption.

4.3.2. IAM Governance Body

Governance of IAM assures that the program is efficient and effective, provides reasonable and appropriate controls, and contributes toward business value and desirable business outcomes. This is driven primarily through the use of forums, which would allow for open discussion between the stakeholders involved in or affected by the IAM program.

4.3.3. Quality Control Prior to Implementation

The foundational technology is centralized directory services. The entire system relies on the quality of the directory information available to ensure accurate data exchange and system access. A system proofing process would provide a system certification and accreditation process prior to joining the central infrastructure.

Due to the large amounts of data handled by several of the larger agencies and IHEs, data clean-up will not be trivial and could require a significant expenditure of resources to accomplish. This effort could be mitigated through careful establishment and enforcement of guidelines and standards to ensure robust data interchange. While this process will require additional resources and staffing, it could be leveraged to significantly improve the overall system assurance levels within the state.

4.3.4. Center of Excellence and On-boarding Support

A number of agencies and Institutions of Higher Education expressed concerns regarding staffing and skillsets related to implementation of centralized identity and access management services. Establishing an IAM Center of Excellence to

centrally establish, leverage and provide examples of best practices and standards would address this concern.

The COE will provide Texas-specific guidance on planning for migration, lessons learned, established best practices and guidance on established standards, including data standards and appropriate points of contact within the state.

4.4. Addressing Cloud Security Concerns

IDaaS is an authentication infrastructure that resides in the cloud. The use of cloud-based services requires the same security diligence as an internally supported infrastructure. The only difference is who is responsible for providing those services.

In considering IDaaS, security standards, requirements, policies, and the vendor's terms and conditions need to be assessed to determine what processes should be implemented to mitigate risk. Maximizing cloud benefits means recognizing that cloud models require unique organizational governance practices to avoid introducing security or regulatory exposures.

4.5 Leverage Existing Architecture for IAM Solutions Currently Deployed

Possible integration of existing IAM investments will have to be carefully managed within the context of the overall state direction due to their variation and maturity levels. While certain aspects and investments made at the agency/IHE-level appear to be mature, they could each be reviewed for opportunities for consolidation and integration as they may require upgrades, maintenance or enhancements.

Several organizations have IAM specific initiatives underway and a number of respondents to the web survey reported having received funding allocations for IAM-specific initiatives (refer to Table 1 below).

Table 1 IAM Specific Funding Received as Reported in IAM Study Web Survey

Agency/IHE	IAM-Specific Funding Received	Project Summary
Texas Health and Human Services Commission	$6,000,000	Implementation and ongoing support of IBM technologies for ISIM, ISAM, TDS, and development of UI for Enterprise Portal
Texas Comptroller of Public Accounts	$1,700,000	Stabilize the current Resource Access Control Facility (RACF) and Active Directory environments. Procure and implement an enterprise single sign-on and password management tool
The University of Texas Health Science Center at San Antonio	$1,000,000	Multi-factor authentication, privileged account management, account management/auditing
The University of Texas Health Science Center at San Antonio	$415,000	Privileged Account Management; Identity Management Core Platform (provisioning); Governance and Analytics
The University of Texas at Arlington	$306,692	Automate account lifecycle for all students, employees, and affiliates access to UTA's IT systems and data.
Tarleton State University	$288,000	DellOne for provisioning and deprovisioning network accounts and providing additional security, along with Dell Password Manager for self-service password support.
The University of Texas at Dallas	$100,000	Migrate from Oracle OIM/HECH to Microsoft Identity Manager
Angelo State University	$15,000	Provide SSO capabilities to ERP system (Banner) without Luminis campus portal.
Sul Ross State University	$11,000	InCommon membership.
Lamar State College - Port Arthur	$3,000	InCommon Shibboleth Federation alliance to allow access within our System (TSU) sister institutions members and others in the future.

5. Bulk Purchase

In accordance with Section 3 of S.B. 1878, DIR was required to conduct a study to develop a bulk purchase strategy across agencies at the lowest cost. If funds are allocated, the department would not be able to utilize the cooperative contracts program due to restrictions in Section 2157.068, Government Code. Agencies would likely have to go out and conduct their own request for offers which would not produce the benefits associated with bulk purchasing.

6. Conclusion

Identity and Access Management as a set of available tools offers organizations the opportunity to pursue IAM components that best fits their needs. The options available to them each offer unique opportunities as well as their own limitations. DIR is prepared to further pursue IAM through a center of excellence as well as preparing numerous implementation options for interested organizations. In the interim, agencies are encouraged to leverage existing IAM options and pursue pilot opportunities where/when available.