State of Alabama

# Information Technology Strategic Plan

Fiscal Years 2017 – 2020

Initial Release v1.0

July 17, 2017

Office of Information Technology

STATE OF ALABAMA

Office of Information Technology

64 N Union Street, Suite 200
Montgomery, Alabama 36130
Telephone (334) 242-3800
Email: jim.purcell@oit.alabama.gov

KAY IVEY
Governor

JIM PURCELL
Acting Secretary

July 17, 2017

The Honorable Kay Ivey
Governor
State Capitol, Room N-104
Montgomery, AL 36130

Subject: Office of Information Technology Overview

Dear Governor Ivey,

I present you with an overview for the State of Alabama Office of Information Technology. In line with the IT Strategic Plan, I'm excited to present you with an overview of our plan to accomplish several critical objectives.

Included you will find documents related to the following:

- OIT Organizational Structure
- OIT Overview
- OIT Services Portfolio
- OIT VOIP Project

I am honored to work with you and State of Alabama leaders to improve the service to our citizens through effective and safe application of technology.

Respectfully,

J Purcell

Jim Purcell

Acting Secretary of Information Technology

## Table of Contents

## EXECUTIVE SUMMARY

The mission of the Office of Information Technology is to

***Make the State of Alabama Government Run***

***Safer, Better, Faster, and Cheaper.***

Our vision for the years 2017-2020 is:

“***To make IT a trusted partner to agencies as they serve the people of Alabama.***

***To reduce redundancies and application costs.***

***Provide a more effective environment for data-driven decision-making.***

***Be more agile in responding to new technologies as they develop,***

***while employing best practices in risk mitigation.”***

To accomplish this, the Office of Information Technology (OIT) must provide IT services that result in effective, reliable and secure operations that meet the state objectives. To this end, the Introduction sets out six technology goals that support this mission.

## INTRODUCTION

In order achieve our vision we must start with an enterprise view of state government and an enterprise view of the technology needed to support state goals. This foundation will be defined as our State Enterprise Architecture. **Enterprise Architecture** is a blueprint of the business of state government, services provided to citizens, strategic goals of the State, and how these goals relate to supporting technologies. It provides an understanding of how technology should support business processes to deliver better services to constituents.

One of the critical concerns of any IT organization, especially State Government, is the responsibility to assure the Confidentiality, Integrity, and Availability of its citizen data. To develop a robust statewide **Cybersecurity** program will require dedicated security resources with the specific training and tools to continuously monitor and prevent or mitigate any attack. To be effective from both a functional and cost perspective, a centralized perspective and resources are necessary. This is an area of vulnerability for the State. Presently we do not have adequate resources in IT with the skills or complete suite of tools necessary to perform this role.

The skills deficit in the area of cybersecurity is part of a broader initiative of **IT Talent Management**. Technology is a rapidly changing field and new skill classifications develop sometimes in months not years.

The current State IT job classifications are more suited to the Mainframe centric, structured programming environment of the 1980's. In addition to redefining the IT classifications, the State needs to be innovative in how we recruit and hire IT talent. The same innovation and "out of the box" thinking that is required in recruiting and hiring must be applied to retention.

**IT Governance and Portfolio Management** will give state leaders an enterprise perspective of our IT investments. The governance process ensures that IT investment decisions are driven by an appropriate life cycle plan from the selection of the project to its ultimate implementation and support. Large IT investments will be managed and reviewed at designated review points so that action on a project that is not meeting expectations can be taken and sufficient remediation plans can be imposed.

The primary responsibility of an **IT Infrastructure** is to provide access, transport, storage and protection of data. It accomplishes this via a connection of numerous electronic devices known as networks. Networks can evolve and become overly complex and inefficient which make them more costly to run and inherently more vulnerable to cyber-attack. The Infrastructure objectives and actions begin the restructuring and simplification of the State network, and network consolidation (where it makes sense).

We cannot protect what we cannot see. Currently, there is not a definitive list of what devices are connected to the state network or a list of software and revision levels that are currently running. To address this gap, **IT Asset Management** is another important piece of the cybersecurity program. Without this fundamental knowledge and the tools to automatically collect and accurately maintain this information in the future, the network will be extremely vulnerable. It is essential that the asset data collected be centrally maintained and regularly updated.

This summary outlines the building blocks to achieve our vision of the IT future state. This is an enterprise vision and it requires an enterprise commitment to succeed.

# ENTERPRISE ARCHITECTURE

**Vision:** To accelerate agency business transformation and new technology enablement by providing a repeatable architecture methodology that is agile and useful and will produce authoritative information of intra/inter-Agency planning, decision-making and management while employing best practices in risk mitigation

Since the beginning of the application of computer technology to business, whether in the private or public realm, there have been discussions of how to improve the alignment of business and technology goals. The perception by Business is that people in IT speak a foreign language comprised of obscure technical terms and often have difficulty communicating with “normal” business professionals.

The reality is that today and into the near future, Business and Technology are inextricably bound. The organizations that will be the most successful are those who have best bridged the gap in management misalignment between business and technology. Enterprise Architecture is a proven framework to optimize Business, Strategy and Technology. The benefits are so substantial that in the public sector, Federal Law and policy require Federal Agency Heads to develop and maintain and agency-wide enterprise architecture that integrates strategic drivers, business requirements and technology solutions. This approach is summarized in **THE FEDERAL ENTERPRISE ARCHITECTURE FRAMEWORK (FEAF) VERSION 2.0**

**Enterprise Architecture** is a blueprint of the business of state government, services provided to citizens, strategic goals of the State, and how these goals relate to supporting technologies. It provides an understanding of how technology should support business processes to deliver better services to constituents.

While the overall magnitude of the problems will be lower for the States, the same drivers still exist: decreasing budgets, increasing customer expectations, external mandates, natural disasters, aging infrastructure, etc. Adoption of an Enterprise Architecture at the State level will yield the same benefits achieved at the Federal Level plus the additional benefit of improving the planning between a State agency and its Federal counterpart. A State Enterprise Architecture based on the Federal EA framework will provide principles and standards for how business, information and technology architectures should be developed across the State so they can be used consistently within and between Agencies, as well as external stakeholders.

This includes an understanding of how central business systems support state operations and ultimately the service providers at the agencies. Enterprise Architecture **documents** the State’s strategic intent, business processes, information flow, supporting technology and the best methods of delivering technology. Enterprise Architecture significantly increases the likelihood for the successful modernization of Alabama’s business systems.

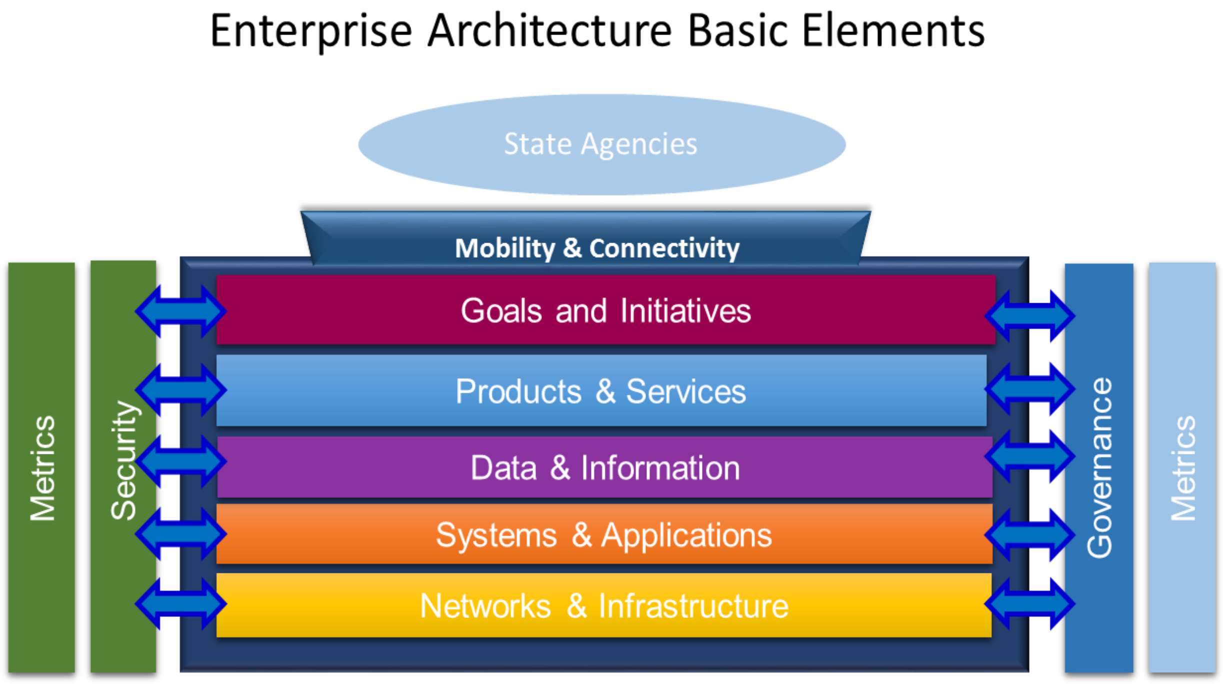
It is not recommended that attempts be made to modernize Alabama’s central business systems in the absence of an Enterprise Architecture. This would be like building a large complex family home with no plans and only verbal input from the teenage children.

Alabama’s current business and technology environment could be characterized as complex and lacking adequate IT-to-business alignment. Agency autonomy and the extent to which Alabama’s business domains (e.g., law enforcement and criminal justice, economic development, financial management, health and human services, education, information technology management, etc.) have technical redundancies across agencies contribute  to complexity. For example, each agency provides for its own technology needs and implements technology solutions that serve often identical business needs across the state, leading to an environment of fragmented data and stovepipe systems.

However, the business processes that support the state do not completely operate within the confines of a single agency’s stovepipe solution. Each stovepipe solution may solve a specific problem, but from an enterprise perspective, it is far from simple or the most efficient solution to deliver state value. It is in this type of environment where the following issues typically surface:

- IT systems become unmanageably complex and increasingly costly to maintain
- IT systems hinder the State’s ability to adequately respond to changing requirements in a timely and cost effective manner (e.g., regulatory changes may require updates to multiple systems).
- Critical Information is consistently out-of-date, incorrect, or virtually impossible to access at an enterprise level.

The integration and purposeful (where it makes sense) consolidation of systems and data, supported by an Enterprise Architecture, will deliver an enterprise view that communicates vital information to executives and decision makers, as illustrated by Figure 1.



Enterprise Architecture Basic Elements

**Figure 1: Enterprise Architecture Framework Meta-model**

## Objective 1.1: Define a set of core artifacts necessary to support Enterprise Architecture.

a) **Action:** Define a set of core artifacts for each sub-architecture that will ensure that future projects will have the information necessary to benefit from the reproducibility of past work.

   a. Sub-architecture domains:

      i. Strategic Goals

      ii. Business Services

      iii. Portfolio Management

      iv. Enabling Applications

      v. Data and Information

      vi. Host Infrastructure

      vii. IT Assets

      viii. Security

b) **Action:** Evaluate and select the necessary EA tools. Work with other State government entities that have begun to implement the FEAF structure and determine which tools have proven to be most effective.

c) **Action:** Determine the Administrative and Technical resources to Administer an Enterprise Architecture Framework

d) **Action:** Prepare a budget plan for tool and resource acquisition

## Objective 1.2: Track progress toward EA implementation.

a) **Action:** Produce an annual report on the status of the EA implementation. The report will become a metric of progress. It will detail the achievements and remaining challenges as well as our IT maturity growth.

# CYBERSECURITY

**Vision:** To make Alabama a leader in cybersecurity among State Governments, integrating security best practices at every level of the Enterprise Architecture and ensuring the confidentiality, integrity and availability of the State of Alabama's IT systems and data are commensurate with mission needs.

One of the critical areas of any organization, especially State Government, is ensuring the Confidentiality, Integrity, and Availability of its information resources that are used to provide infrastructure support and services. Government systems are inherently under attack from the outside, besieged not only by the hacker intent on demonstrating technical prowess but also by other entities like political activist organizations bent on influencing political outcomes, criminal syndicates focused on generating revenue by stealing data, and external Nation States whose purposes and goals are perhaps the most varied and nefarious. With these threats in mind and in consideration of various internal threats, we in State government must endeavor to embrace our responsibility for establishing and maintaining the trustworthiness and efficiency of Alabama's Information Systems, Services, Business Processes, Missions, Organizations and apply due diligence to the management and oversight of State information resources. However, at this time there is no specific Alabama standard or law that provides a path to addressment of risks and threats to our systems and resources.

In response to a recognized need to bring oversight and purposeful direction to the issues, the OIT Strategic Plan published in April 2014 established a strategic goal of adopting a risk-based approach to IT resources management. Later, in December 2014, the Secretary of Information Technology issued a memorandum declaring IT Governance as a "vital management structure" that could benefit the State through "improved business processes and [the realization of] efficiency savings." Then again, in September of 2015, the Secretary of Information Technology released a Memorandum instituting development of an OIT Information Security Program based upon the "formal adoption of the National Institute for Standards and Technology's Risk Management Framework." In the same month, the Governor issued a proclamation with matching wording: "formal adoption of the National Institute for Standards and Technology's Risk Management Framework."

With the decision to model a process developed by the Federal government comes a significant challenge to make these concepts relevant and consumable by the agencies of the State of Alabama. In response to the declarations and requirements, and in line with the concepts presented in NIST Special Publication 800-39, the OIT Office of the CISO has developed the following as objectives in initiating the journey to achieving the original strategic goal of creating and implementing a risk management based information security program:

## Objective 2.1: Establish appropriate governance structures for managing risk.

a) **Action:** Ensure that senior leaders & executives recognize the importance of managing information security risk.

b) **Action:** Establish Authoritative Governance to require:

a. Accountability & Responsibility structure for Security Responsibilities at the agency, business unit, system, information, and system component levels

b. Definition of Agency Missions, Strategic Goals, Objectives, & Priorities

c. Development and publication of acceptable Architecture Reference Models for all levels of Enterprise Architecture (to include Segmentation Architectures, Solution Architectures, Mission & Business Processes, System Boundary requirements, etc…)

d. Definition & Application of logical & physical system boundaries, enclaves

e. Information Systems developed, architected, engineered, & acquired according to a System Development Life Cycle with Security Engineering Principles built-in

f. Allocation of Security Controls to agency Information Systems (Minimum Protection Standards)

## Objective 2.2: Ensure that the State's risk management process is being effectively conducted at the Agency, mission/business process, and information system levels.

a) **Action:** Develop a set of Minimum Protection Standards applicable to all Alabama Information Systems.

b) **Action:** Develop State-wide Cybersecurity Program Management framed on the 16 NIST 800-53 Program Management components

c) **Action:** Develop State-wide policies and standards that allow for the proper application of the State Minimum Protection Standards structured off of the NIST Special Publication 800-53 Security Controls Families, Controls, and Enhancements.

d) **Action:** Aid agencies in the understanding and implementing the requirements of the OIT Cybersecurity Programs and in the development of their own more specific standards and documentation that adhere to the Statewide Minimum Protection Standards:

   a. Agency Program Management development (NIST SP 800-53 Appendix G)

   b. Agency Security Control application (NIST SP 800-53 Appendix F) for common language among the State Cybersecurity culture

e) **Action:** Develop a "Knowledge Service" website that provides guidance, education, direction, etc. that will aid agencies in the development of their Security Programs and Program Management.

f) **Action:** Establish a centralized Security monitoring and response capability. Identify the tools, staffing, training and other requirements and determine the budget to support this capability.

## Objective 2.3: Establish a Statewide culture that considers information security risk during the design of mission/business processes, enterprise architecture, and system development lifecycle processes.

**a)** **Action:** Develop State Enterprise Architecture-based Security Reference Architectures to be used as guidance throughout a system's development lifecycle that:

**a.** Requires clear Mission and Business Process definitions

**b.** Requires clear system boundaries & appropriate segmentation architectures

**c.** Requires system component baseline security configurations

**d.** Requires business continuity and contingency planning concepts

**e.** Defines architectures for specific solutions

**b)** **Action:** Develop State-level and agency-level risk management strategies that address how the State and State agencies intend to assess, respond, & monitor risk and that specify assumptions, constraints, risk-tolerance, and priorities/trade-offs used within the State and State Agencies for making investment and operational decisions.

## Objective 2.4: Develop and clarify the risk management responsibilities of individuals accountable for systems development, implementation, or operation.

a) **Action:** Establish Responsibility and Accountability structure as it applies to managing risk in the design, development, implementation, operation, and disposal phases of the System Development Lifecycle (OR as they apply in the Tier model of RMF)

b) **Action:** Ensure compliance with mandated Statewide General Cyber Security Awareness Training in line with Alabama IT Security Program Plan

c) **Action:** Implement Statewide Specialized Cyber Security Training in line with Alabama IT Security Program Plan

d) **Action:** Establish Specialized Cyber Security Job Classifications in line with Alabama IT Security Program Plan

e) **Action:** Collaborate with Agency security professionals to ensure understanding, acceptance, and timely implementation of cybersecurity policies and best practices.

f) **Action:** Establish a process to communicate Security topics such as new malware development, recent scams, special topics, etc.

Successful adoption and utilization of RMF at the information system level will require a top-down approach and a thorough understanding of the NIST-based Federal model. OIT leadership, vision, and buy in to purposefully mandate introduction of risk management concepts into the State culture and drafting of cybersecurity legislation to create an accountability structure for managing risk to State information resources through the creation of a specific organizational role structures will ensure that the Cybersecurity Program management controls, security control language, and risk-assessment concepts are appropriately architected as necessary for agencies to fully utilize the intent and benefits of NIST developed guidance as a common language to assess and manage risk in Alabama systems.

# IT TALENT MANAGEMENT

**Vision:** To cultivate an I.T. staff / team that effectively supports and drives agency security, service, and innovation.

IT Talent Management is a critical strategic initiative because the State has an aging workforce that will be retiring and taking with them a tremendous amount of intellectual capital regarding state processes and systems. Technology is a rapidly changing field and new skill classifications develop sometimes in months not years. The current State IT job classifications are more suited to the Mainframe centric, structured programming environment of the 1980's. Most Universities have dropped from their core curriculum classes required to meet many of the job classifications currently used by the State. If we are to succeed in meeting the OIT vision for the State, then we need to ensure that we can hire the specific talent we need. It is essential to update the IT job classifications to match the technology needs that we have today and that they be maintained on an ongoing basis to ensure that the classifications continue to evolve as technology and associated skills change.

In addition to classifications, the State needs to be innovative in how it recruits and hires IT talent. Unfortunately, it is not always possible to predict technology resource demand as accurately as required to fit an annual planning cycle. Demands placed upon the State often require a rapid technological response and there is a need to meet these challenges with innovation and agility in resource acquisition that will allow the IT organization to meet these expectations of the State.

As challenging as recruiting and hiring IT talent may be, it will be less than successful if the talent that is hired is not retained. The same innovation and "out of the box" thinking that is required in recruiting and hiring must also be applied to retention. IT personnel make up a unique workforce. They are motivated by technical challenges and receive job satisfaction in resolving those challenges. While salary advancement is a basic need, it is the opportunity for professional growth and broadening of technical skills that is a prime motivator in job appeal. There is a large percentage of this workforce that does not aspire to people management but are often forced in that direction because it is the only path to career progression. The result is often the loss of a good technologist and the creation of a less-than-effective manager. Consideration must be given to the development of multiple career ladders that would include both a technology and a separate people management track.

## Objective 3.1: Work with the State Personnel Department to ensure any state personnel classification system for IT positions is current, aligns with the business needs of the state, and is reviewed annually and updated as required.

a) **Action:** Conduct an IT Talent Study to update and enhance the IT job classifications to align with current and projected skills needs.

b) **Action:** Develop a technologist and management career path that requires relevant education and certifications for career growth.

c) **Action:** Develop an on-going process to annually monitor, assess and revise the state IT job classifications.

## Objective 3.2: Work with the State Personnel Department to develop an IT Talent sourcing approach to accomplish both long and short-term technology goals.

a) **Action:** Conduct a market assessment to understand skill availability and salary trends for the updated IT job classifications.

b) **Action:** Define the appropriate roles to be filled by an employee staffing plan, staff augmentation, and Service/Project Outsourcing.

## Objective 3.3: Work with the State Personnel Department to develop a compensation structure that allows the state to compete effectively for IT personnel with the necessary skills to meet the Technical needs of the State.

a) **Action:** Conduct a market rate study to update IT salaries to current market rates.

b) **Action:** Develop an on-going compensation review process that periodically calibrates state IT salaries with comparative public sector rates for similar skills and responsibilities.

## Objective 3.4: Work with State Personnel to develop an IT application process that is simplified, responsive and facilitates qualified candidates in applying for state IT opportunities.

a) **Action:** Streamline the online application process.

b) **Action:** Develop guidelines and encourage agencies to use the State Intern and the State Professional Trainee classifications to recruit and attract college students and recent graduates.

c) **Action:** Provide a mechanism for IT testing services that can be customized to match position requirements.

d) **Action:** Re-examine the current policies on hiring contract personnel into permanent positions commensurate with their experience and salary level.

## Objective 3.5: Update the staff augmentation contract to enable broader vendor participation and more flexibility in acquiring specialized skills.

a) **Action:** Develop a contract for a managed service provider to manage the process and vendors supplying supplemental IT staffing.

b) **Action:** Develop an on-going process to periodically monitor, assess and revise the contract IT job without requiring a new ITB or RFP.

### Objective 3.6: Develop professional development plans that offer career progression paths and encourage continuous skills enhancement and update.

a) **Action:** Define career paths to technical specialists, managers and CIO's.

b) **Action:** Develop professional development plans that can be customized to match employee aptitude and agency needs.

# IT GOVERNANCE AND PROJECT PORTFOLIO MANAGEMENT

**Vision:** Individual and collective technology investments that meet stakeholder needs, drive state and agency strategy, and minimize risk.

IT Governance, like Cybersecurity, is involved in every phase of EA. The governance team ensures that everything works by appropriate life cycle plan - from the selection of the project to its ultimate implementation and support. They are not an operational group per se, but verify that each operational group has performed its role. They consolidate all of the documentation and ensure transparency to all of the stakeholders by providing a regular report and scorecard on governed projects. They can, at designated review points, take action on a project that is not meeting expectations and impose a range of actions including putting a hold on the project until a sufficient remedial plan is accepted. Figure 2 depicts the interactions of the Governance committee with other organizational entities.

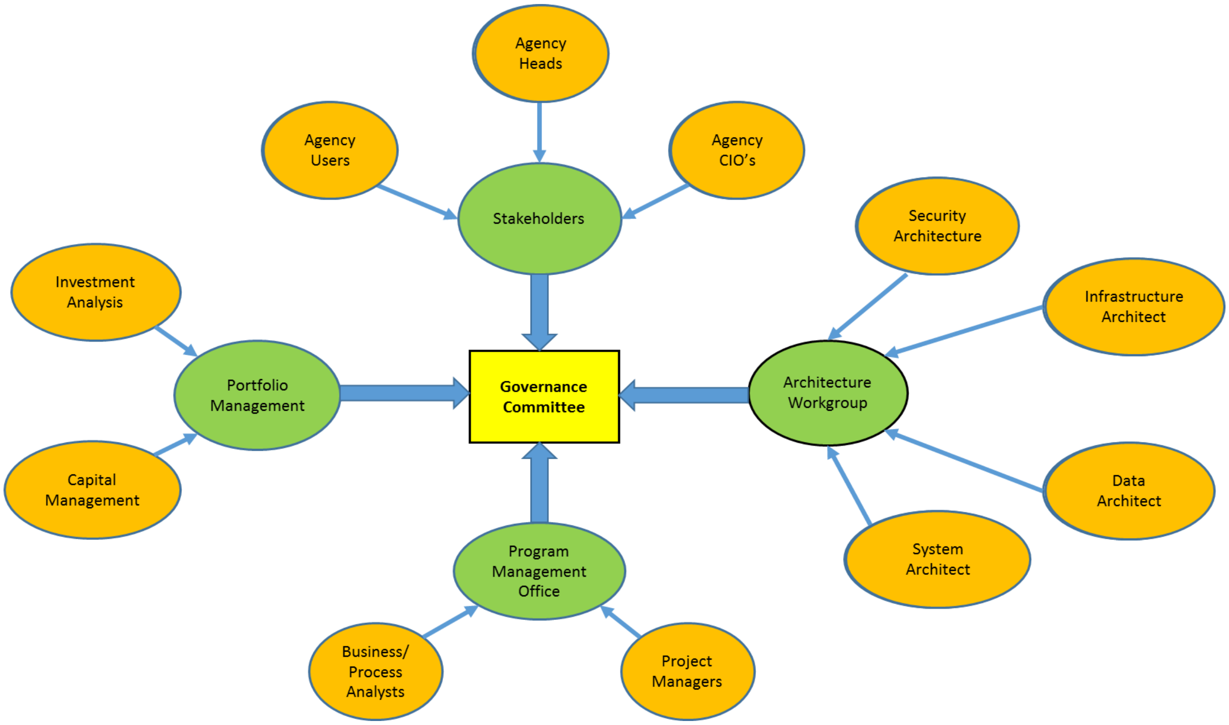


**Figure 2: Governance Committee Interactions**

Figure 2 also shows that because of the complexity of interactions, the Governance Committee, like Cybersecurity, is a centralized group performing this service for all agencies. In addition, to be noted is that this figure also identifies many roles that do not exist in today's IT structure, such as the Architecture Workgroup which would also be a centralized resource to serve all agencies.

Another role of the Governance Committee is to work with investment analysts and document each project's return on investment and risk assessment. Each project's risk will vary due to its complexity and utilization of new technology. The Committee will work with the agencies to ensure an optimum mixture of projects that maximize return and minimize risk.

## Portfolio Management

### Objective 4.1: Implement a Project Portfolio Management Methodology.

a) **Action:** Utilizing Strategic Planning resources work with agencies to develop a three-year strategic Plan and document these plans for each agency.

b) **Action:** Define the PPM Process:  Scope, long- and short-term strategic goals, and processes required to attain those goals

c) **Action:** Identify the tools and technologies that support the processes; identify processes that work and revise or eliminate those that don't

d) **Action:** Develop a process to qualify and rank projects based on their investment return, complexity and business criticality in order to ensure the optimum selection of projects consistent with the State's strategic needs.

## Project Governance

### Objective 4.2: Establish a Project Governance Structure.

a) **Action:** Establish the composition of the Governance Committee (staffing levels, etc.) and define its relationships to other stakeholder areas.

b) **Action:** Ensure statewide adoption and use of the Project Governance policies, which provide an oversight function for critical projects – reviewing and approving each phase of such projects to ensure that it meets the defined needs of the stakeholders.

c) **Action:** Ensure that significant IT investment projects align with statewide strategic direction and organizational objectives

d) **Action:** Identify and acquire automated tools to collect and store all project artifacts that will also provide analysis and reporting on project status.

### Objective 4.3 Establish Statewide, Standardized Project Management Tracking

a) **Action:** Determine measures meaningful to project stakeholders

b) **Action:** Be transparent; communicate; distribute project information; establish a culture that encourages open and honest reporting

c) **Action:** Implement key performance indicators (KPIs) that lead to improving the practice of Project Management.  KPIs help to monitor progress, determine how and when to take control to correct a process, and provide a means to measure success.

## IT Infrastructure

**Vision:** Establish a Cost Effective, Secure, Reliable, and Scalable IT Infrastructure that Supports the Business Needs of State Agencies.

Ultimately, the business of IT is data. As State employees utilize software applications, they cause data to move to and from places of storage to other places such as a PC where data can be viewed or modified or to a printer where it can be read. The core structure that allows data to move is the network - a collection of wires, hubs, switches, routers, wireless transceivers and transmitters, etc. that transport data to its intended destination. Just like a highway system, it must be managed. Try to send more data than the network was designed for and performance suffers. Data storage is not infinite. There is a cost for storage, whether on premise or in the cloud. In addition, it has to be managed in such a way that it allows for the free flow of data but is able to detect and destroy any malicious packet of data and ensure that no unauthorized user can access or view data.

Infrastructure is the basic collection of electronic Legos that is fundamental to the operation of an IT organization. Just like Legos, you build very efficient designs or you create convoluted, inefficient structures that work, but cost more to maintain and, more importantly, increase the vulnerability that the network could be breached by an unauthorized user. This situation becomes more complex when we look at Figure 3, which shows that the State network is not a single network but multiple interconnected networks managed by different State agencies. The Infrastructure strategies and objectives propose a plan to begin the restructuring and simplification of the State network and purposeful consolidation (where it makes sense to the state and agencies).

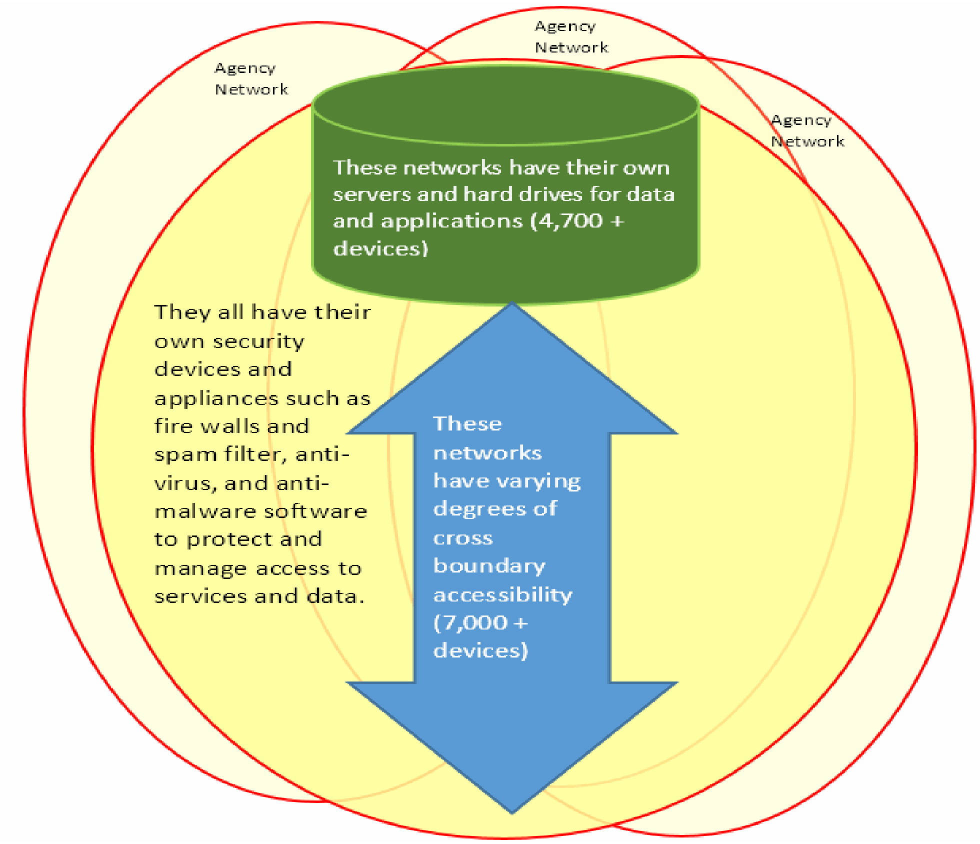

Agency Network
Agency Network
Agency Network
These networks have their own servers and hard drives for data and applications (4,700 + devices)
They all have their own security devices and appliances such as fire walls and spam filter, anti-virus, and anti-malware software to protect and manage access to services and data.
These networks have varying degrees of cross boundary accessibility (7,000 + devices)

**Fig 3.0 Current State Managed Networks**

## Objective 5.1: Ensure availability and access to reliable and scalable computing resources and IT services.

a) **Action:** Adopt a “cloud-first” policy and establish governance for cloud services use.

b) **Action:** Establish a hybrid state cloud that may incorporate multiple commercial cloud offerings, while utilizing the state’s existing investment in on premise infrastructure where justified.

c) **Action:** Migrate applications and data to the cloud when it can provide the state the most security and value.

## Objective 5.2: Maximize efficiencies and reduce data center operating costs while minimizing risk.

a) **Action:** Establish standards and enterprise governance for the operation of Data Centers.

b) **Action:** Consolidate computing and storage resources to secure data centers driven by security categorizations, where it makes sense, so that maximum efficiencies can be realized.

### Objective 5.3: Establish a secure network infrastructure that successfully supports the delivery of services to the state, while providing a level of flexibility and scalability to support the introduction of new and innovative technologies and services.

a) **Action:** Design, develop, and implement a secure, integrated, flexible, and robust network infrastructure that supports the delivery of services to agencies and citizens.

b) **Action:** Integrate security technologies that allow for the unified management of network security policies and services.

c) **Action:** Implement robust network monitoring, supported by automated tools that provide an integrated view of the network enterprise that allows for control and security.

### Objective 5.4: Enable user security, user mobility, standardized employee profiles for IT setup based on job roles, consolidated reporting, and unified management of end user devices.

a) **Action:** Develop and implement a statewide, unified, and integrated Identity and Access Management (IAM) that will provide a global, common, automated and secure repository for trusted identification.

b) **Action:** Centralize the overall administration of the state's Identity and Access Management while providing lower level administration for agency Managers.

c) **Action:** Implement multifactor authentication across the enterprise where it makes sense.

## IT Asset Management (ITAM)

**Vision:** To provide a knowledge base of IT Asset information that will support the Business, Technological and Security needs of the State.

It may seem curious that IT Asset management is a key portion of the state IT strategic plan. We have an audited State Asset list but this is created on a financial basis. It does not contain leased products or products under a certain dollar amount. To meet the security and technology planning needs of the state, IT Assets are any device connected to the network. These assets may be a switch, router, or terminal, a leased item, or software. The dollar value is not one of the critical attributes of the IT list because it does not matter what the item cost, but what impact it has on the network with respect to performance, security and total cost of ownership.

Currently, there is not a definitive list of what devices are connected to the state network or a list of software and revision levels that are currently running. Without this fundamental knowledge and the tools to automatically collect and accurately maintain this information in the future, the network will be extremely vulnerable. One of the things that hackers regularly exploit is software with a known deficiency that has not been upgraded or data collection access points such as point of sale scanners.

While some initial work has been completed in collecting this IT Asset data, this collection must be completed, whether by manual or automated discovery methods, for all networks. Currently the State has no automated discovery tools but product evaluation is underway.

It is essential that the asset data collected be maintained and regularly updated in a centralized database. In the future, with cross-reference data such as serial number, it may be possible to provide the IT data to the State Asset Management database, saving time and money on Annual Audits.

### Objective 6.1: Implement an asset discovery process to identify and provide information to manage state's IT assets.

a) **Action:** Implement Simple Network Management Protocol (SNMP) to allow automatic query of network enabled devices and obtain hardware and software data for all devices on the network.

b) **Action:** Implement asset discovery process to automatically discover and inventory infrastructure/network devices, appliances and firmware versions.

c) **Action:** Identify and record additional hardware and software assets connected to a State network not captured thru SNMP.

d) **Action:** Identify non-networked IT related hardware and software.

### Objective 6.2: Reduce costs to the State and agencies for IT related asset acquisition and maintenance.

a) **Action:** Initiate a prototype to test tools and procedures for IT asset data collection.

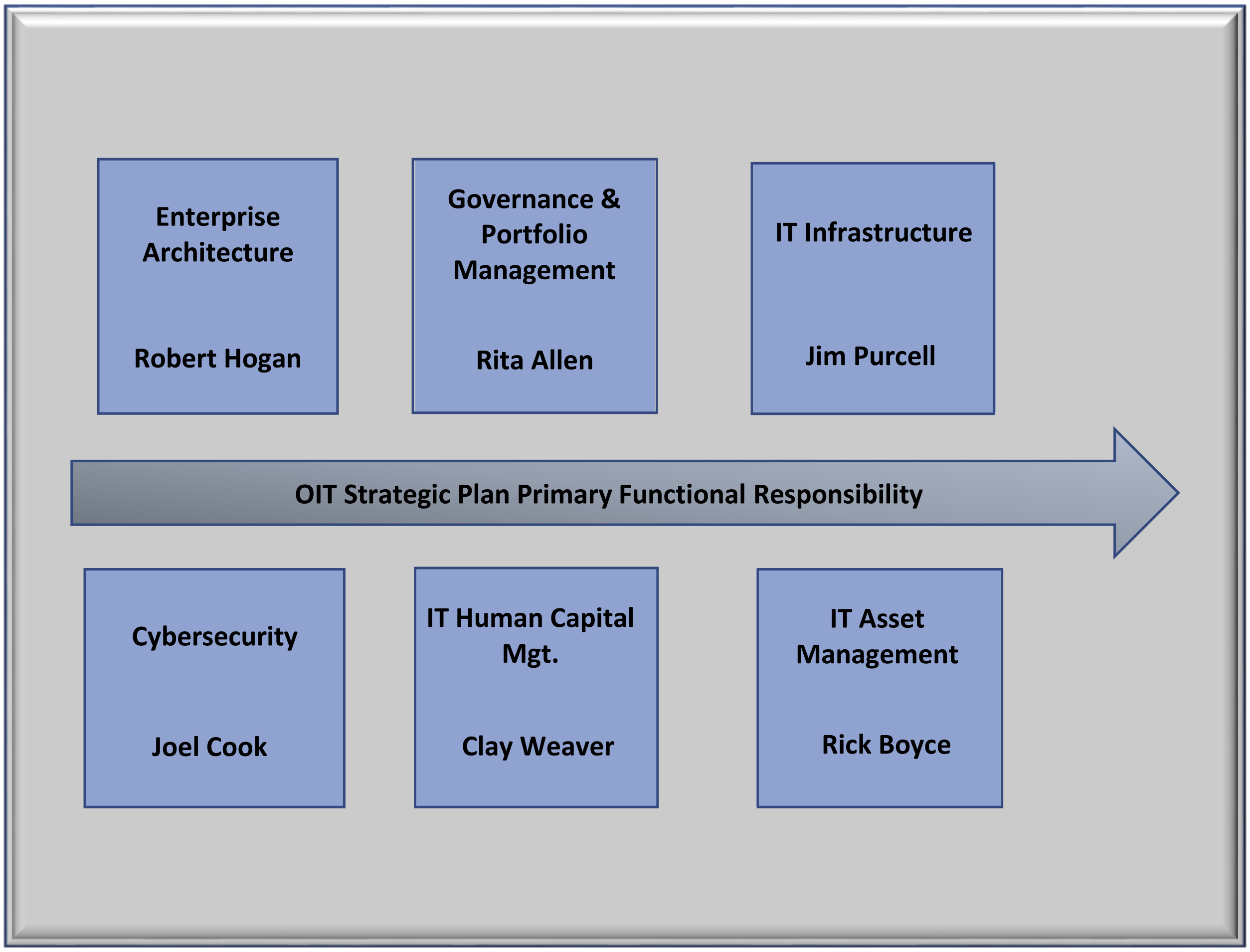
b) **Action:** Develop a roadmap for Statewide rollout

c) **Action:** Compare final IT asset database to the IT Audit database and resolve discrepancies

d) **Action:** Develop a process to ensure that all new IT assets acquired are loaded to IT asset database with the required data attributes.

# APPENDICES

## Appendix 1:  OIT Strategic Plan Functional Responsibility



Enterprise Architecture

Robert Hogan

Governance & Portfolio Management

Rita Allen

IT Infrastructure

Jim Purcell

OIT Strategic Plan Primary Functional Responsibility

Cybersecurity

Joel Cook

IT Human Capital Mgt.

Clay Weaver

IT Asset Management

Rick Boyce