



Office of Information Technology Services

ANDREW M. CUOMO
Governor

MARGARET MILLER
Chief Information Officer

November 22, 2016

By Electronic and U.S. Mail

John Buyce
Audit Director
Office of the State Comptroller
Division of State Accountability
110 State Street, 11th Floor
Albany, NY 12236

Re: *"Effectiveness of the Information Technology Transformation"*
Report 2015-S-2

Dear Mr. Buyce:

I write to respond to the Office of the State Comptroller's ("OSC") Final Audit Report, Effectiveness of the Information Technology Transformation, dated August 24, 2016. On behalf of the Office of Information Technology Services ("ITS"), and pursuant to Executive Law § 170, I write to provide additional information to clarify and expand ITS' responses to OSC's four recommendations in the Final Report.

OSC Recommendation 1: Formally assess the adequacy of the internal control environment at ITS and take necessary steps to ensure the control environment is adequate, including cooperation with authorized State oversight inquiries.

ITS Response:

ITS is committed to establishing and maintaining a comprehensive system of internal control throughout the agency. A strong internal control system provides reasonable assurance that the agency will achieve its mission and objectives in an effective and efficient manner in compliance with existing laws, rules, and regulations, and to enable cooperation with appropriate third parties.

The Internal Controls Office ("ICO") within ITS maintains a comprehensive internal control review program for the agency. Pursuant to the requirements of the *New York State Governmental Accountability, Audit and Internal Control Act* of 1987, ITS developed the program using the COSO Framework; the program adheres to the Office of the State Comptroller's *Standards for Internal Control in New York State Government*. The program includes an annual formal survey of all five components of internal control. The ICO provides executive management a report of the results of the formal survey on an annual basis and the ICO and management discuss areas where actions could be taken to strengthen internal controls. The entire executive leadership team reviews results to ensure necessary steps are taken where required.

Consistent with its mandate and with its annual assessments of the ITS control environment, the ICO assists numerous units in creating procedures to formally document their functions and processes. Agency management frequently seeks advice from the ICO on how best to strengthen existing controls in place, identify and remediate internal control gaps within processes, and perform more effective monitoring activities. The ICO works with functional management to develop tests of controls in place, determine the source of any control weaknesses or inconsistencies identified, and develop a suitable remediation plan to strengthen controls. The ICO reviews agency policies, standards, and guidelines for potential control opportunities, conflicts, and gaps to ensure efficient, effective, and transparent operations.

ITS executive leadership understands its responsibility for setting the agency's expectation for internal controls, ensuring management is aware of those expectations, evaluating management's effectiveness at maintaining and supporting the system of internal control, and cooperation with authorized third parties concerning the ITS control environment.

OSC Recommendation 2: Complete an overall risk assessment of ITS and incorporate it into the new FY 2016-17 project plan.

ITS Response:

Operational Risk

The ITIL® (Information Technology Infrastructure Library) Maturity Model is an industry model for IT service management and delivery, which involves an assessment of processes, automation, communication, and coordination of an IT organization, as related to security, service and cost, as those elements impact the delivery of IT services and customer experiences. The ITIL framework enables identification and mitigation of risk while enhancing processes. The 26 ITIL processes address service strategy, service design, service transition, service operation, and continual service improvement.

Use of the model facilitates process improvement in conjunction with identification, assessment and mitigation of risks that are tied to the success of the ITS mission, which is to create and deliver innovative solutions that foster a technology-enabled government to best serve New Yorkers.

Pre-consolidation, the maturity level of IT organizations within disparate agencies varied. ITS evaluated its services against the ITIL model, and determined that, as a whole, the agency aligned with the initial level of maturity (level 1), which is the least mature. Over the last two years, ITS has focused its efforts on driving service delivery to level 2 (Defined) for key processes. This multi-year initiative will continue to drive up the maturity curve to reduce operational and security risk and deliver best value for the taxpayer.

In partnership with the Division of Budget and customer agencies, ITS also created and uses its project portfolio process to assess, prioritize, and address technology risks as part of its investment criteria. The project portfolio process flags critical risks and prioritizes projects designed to mitigate them, enables modernization, and facilitates sharing of appropriate technological improvements across multiple agencies. The process also mitigates risk by ensuring the total cost of technology ownership is included in the budget request, which will prevent accrual of a future technology debt.

The ITIL® assessments have led to evaluation and re-engineering of key operational processes: Incident Management, Change Management, Service Request, Configuration Management, and Problem Management. Those assessments flagged various operational risks, and led to structural and process changes that mitigate and remediate identified risks.

In addition, specific risk assessments for the consolidation of data centers is ongoing. These assessments examine facility exposures and operations processes, and also evaluate servers, hardware standards, patch levels, and impacted applications, among other criteria. The resulting threat scores enable prioritization for high risk/high threat sites, as well as the execution of mitigation strategies to target specific risks/threats identified.

Cyber Security Risk

The Enterprise Information Security Office (EISO) has a robust, multi-faceted risk management program, aligned with the industry best practice standards of the National Institute of Standards and Technology Security and Privacy Controls for Federal Information Systems and Organizations (known as NIST 800.53) and ISO 27001 (the Information Security Management standard). Below is a general process overview, followed by a brief summary of ongoing assessments:

1. Identify core competencies and mission-critical business functions;
2. Inventory assets (data, systems, infrastructure) that support core competencies and mission-critical business functions;
3. Identify statutory/regulatory compliance requirements;
4. Understand technical security requirements;
5. Select/tailor controls;
6. Implement, test and validate controls;
7. Manage emerging risks through security audits/reviews, change and configuration management, and vulnerability scanning.

There is currently a project underway focused on application risk assessments for those applications that are critical to customer agencies operations and/or involve Personal, Private, Sensitive Information (PPSI), are external-facing, or otherwise identified by the Chief Information Officer or agency Commissioners. The project institutionalizes a standardized approach to identifying, triaging, prioritizing, assessing, and remediating risk issues, and also supports the development of disaster recovery plans. The EISO comprehensive assessment process provides a holistic view of risk that includes business, regulatory, and technical perspectives, with comprehensive technical controls reviewed. In addition, EISO, in conjunction with the Chief Operations Office, is driving an asset inventory, which will support a technical assessment of risks related to software, versions, and support status.

These assessment efforts drive risk-based decisions, investments, and strategic planning for ITS. They ensure that ITS leadership prioritize resources and projects so that the agency can effectively, efficiently, and securely provide IT support to Executive Agencies. The information technology industry is replete with known threats and emerging risks, which demands that we remain vigilant in our organizational, operational, and cyber

security risk assessments, and stay poised to promptly address the threats and vulnerabilities that give rise to risks.

OSC Recommendation 3: Establish formal timelines for completing various phases of Transformation projects and the broader Transformation itself.

ITS Response:

The transformation program as described in the SAGE report was scoped as follows: "... a comprehensive overhaul of the State's information technology functions. This transformation can be divided into three parts: a reorganization of the way in which the State manages the IT function; modernization of the State's IT infrastructure; and acceleration of the development of IT projects with a high return on investment and a high impact on performance."

This response focusses on the progress to date in each of the 3 areas as scoped in the SAGE report.

We make multi-year plans based on the best information available at the time while continuously modifying these plans as the needs of citizens and agencies evolve, as we learn more about the environment and as circumstances demand.

Our plans are informed by the imperative of recognizing significant fiscal constraints across all state agencies, ensuring we're spending smart on those initiatives that deliver maximum citizen impact, are closely aligned with administration and agency goals and that return on investment (both financial and mission) is maximized.

1. Reorganization of the way in which the State manages the IT function

While we will continuously seek to improve our management of the IT function as needs demand we consider the original scope complete. This has been achieved in the following ways

- Consolidation of IT budgets and personnel into a single agency serving the IT needs of those executive agencies within the scope of ITS.
- Authority of the CIO and ITS over the IT functions for these agencies.
- Creation of standard policies and technology standards
- Establishment of a strong, centralized Program office which has established project management standards and a strong portfolio management process. Specific achievements in this area includes the following.
 - Coordinated enterprise wide IT Investment planning identifies where multiple entities requesting duplicative or similar new business capabilities and technology platforms, presenting opportunities to share solutions and standardize technology.
 - Prioritization of and persistent focus on technology remediation has resulted in significant progress in decreasing the technical debt accumulated from years of underinvestment in IT infrastructure.
 - Project investment planning has been re-engineered with a heightened emphasis on project financial components including annual operating costs.
 - The annual IT investment planning cycle is supported by demand portfolio software to streamline capture of IT Investments requests, and sharing with stakeholders including agency finance offices and DoB Examiners.

2. IT Infrastructure Modernization

The SAGE commission identified four major, enterprise-wide projects, as key to this aspect of the Transformation program. These four projects are: (i) upgrading the State's data centers; (ii) replacing analog phone networks with consolidated digital networks that include voice over Internet protocol (VoIP); (iii) standardizing and integrating email; and (iv) implementing enterprise-wide identity and access management for the State's major software applications.

Data Center Modernization

The Tier 3 data center specified in the SAGE report has been built at the Center for Nanoscale Engineering (CNSE). To date the systems formerly housed in 24 legacy data centers have been migrated into the CNSE. In 2017, another nine in scope legacy data centers are scheduled to be migrated as financial circumstances allow, at which point this scope will be complete. Over 90% of the server infrastructure at CNSE is now virtualized, which far exceeds the industry standard.

We are making use of public and private cloud services as appropriate to the needs of each service in order to achieve the optimum cost and security profile in each case.

Digital Network Consolidation

As of November 2016, over 65,000 phones have been migrated to the VOIP service outlined in the SAGE report. These include remediation of the network infrastructure at every site, which is a pre-requisite to offering digital voice communication. The project to migrate legacy phones to VoIP is in the closeout phase and will end in 2017.

There are still approximately 4,000 phones which will remain on current technologies, as migrating to VOIP technology would not be cost effective. These phones are primarily at locations where either adequate network infrastructure is not available or has less than 10 phones needed. It will require extensive upgrades or modernization of the current network infrastructure at these sites to offer VoIP phones which would not be cost effective. As part of the routine upkeep of these remote sites, if the State refreshes the network infrastructure, ITS may convert the telecommunications at these locations to VoIP in the future. For any new site that an agency may occupy, ITS will evaluate the network infrastructure on a case by case basis, and implement the optimal network and telecommunication solution.

Email Consolidation and Integration

When ITS was created there were 22 email systems in use across the Agencies within ITS's scope. All of these disparate email systems have been successfully decommissioned and approximately 164,000 mailboxes migrated to a single, hosted email system. This project is now complete.

Enterprise Identification and Access Management

ITS has taken a holistic approach with the goal to establish a common enterprise user identity store and meet NYS security and compliance requirements for the State agency users, citizens / businesses of NYS. The approach ITS laid out and has been working on needs to enhance the security posture of the current infrastructure that supports many complex legacy applications including DMV and Tax with millions of user accounts, while building a new enhanced solution. As with other projects, prior to IT transformation, each agency adopted various business processes, technology solutions and implementation approaches. ITS has divided the effort into two sub-projects:

1. Active Directory (AD) consolidation for all 130,000+ NYS Users

ITS has standardized Microsoft Active Directory as the technology for all NYS users thus offering ability to provide single sign-on capabilities for all the 130,000+ end point devices. As part of this effort, ITS is in the process of consolidating over 50 agency Active Directory (AD) domains supporting state employees' identity into one Enterprise Active Directory domain. This will enable ITS to reduce infrastructure and operational costs associated with maintaining these domains and provide enhanced security and audit capabilities. In addition to AD consolidation, ITS is enhancing security for users with the roll-out of over 100,000 tokens for multi factor authentication for critical applications starting with email and VDI.

2. Remediation and Enhancement of NY.GOV ID – service used by millions of citizens to access critical services such as DMV, Tax and other online Human Service systems.

NY.GOV ID has approximately 11 million user accounts. Limitations of the legacy systems and the complexity involved in achieving the goals of this project require a careful approach be taken. Prior to adding functionality to the NY.GOV ID service, ITS took the first step to upgrade the underlying software and infrastructure. Over the past two years, significant progress has been made to establish a common foundation with most current supported versions of software and hardware. This foundation enables us to migrate business applications to the new platform.

Building on the stable foundation, ITS is using a three phase approach to clean-up the directory, and also offer additional features and functions. This is a massive project that will be developed while maintaining the existing process that are in place to serve the needs of New York's citizens, businesses and visitors. Its complexity is matched by the opportunity to save money, improve resiliency, audit and availability.

Phase 1: Built the Enterprise Identity Store Foundation to streamline account provisioning and de-provisioning, password reset self-service etc. (Estimated Completion: Spring 2017.)

Phase 2: Establish Privileged Account Management Solution to provide enhanced access control and audit of system access (Estimated Completion: 2017). The team is working closely with OSC Payroll team to enable self-service for looking up payroll stubs online, and enable additional security to allow updates to personal information online. Both of which is a big step forward, in offering convenience to State employees and reducing the administrative cost involved in printing and mailing the stubs.

Phase 3: EIAM Phase 3 will build upon the prior phases and deliver an integrated enterprise identity management capability to be leveraged by all NYS business applications. ITS released the RFP (PBITS) to acquire system integration services on 11/8/2016. Upon selection of a system integrator, we expect to take three to five years to migrate all users and legacy business applications to the new platform.

3. Acceleration of the development of IT projects with a high return on investment and a high impact on performance

As described above, ITS have established a strong, centralized Program office which has established strong portfolio management process. Project investment planning has been re-engineered with a heightened emphasis on project financial components including annual operating costs and return on investment in terms of both financial return and mission alignment. The proposed portfolio of projects submitted annually by each agency is reviewed by DOB for affordability, and by Commissioners and Deputy Secretaries to ensure mission alignment and priority. This rigorous portfolio planning and review process ensures resources are expended on those projects with the highest impact on priority goals. Priorities will evolve over time but the

mechanisms required to ensure the achievement of the original goals are now in place. The sample projects listed in Exhibit 14 of the SAGE report were purely illustrative. The portfolio agreed with Agencies, DOB and Chamber replaces this sample list. We consider this scope to be complete.

OSC Recommendation 4: Work with state agencies to facilitate their sharing of successful and innovative practices to more efficiently and effectively manage ITS resources and assets.

ITS Response:

ITS, as the sole IT provider for its supported agencies, has the unique advantage of seeing the best practices across the State as they evolve. ITS already has several avenues to facilitate the sharing of successful and innovative practices to more efficiently and effectively manage ITS resources and assets. Several functions and organizational units within ITS carry out the critical role of agency specific and enterprise wide collaboration.

As described earlier, NYS IT Portfolio Management process offers a vehicle for State agencies to work closely with ITS Cluster executives to develop IT Investment Requests (ITIRs) which documents the business problem an agency is trying to solve. Each Agency works closely with cluster staff to develop ideas about the use of technology solutions to meet the Agency's strategic goals.

Enterprise Platform and Business Solutions group is taking technologies that were deployed across one or more agencies, standardizing them and centralizing the staff into logical or physical communities of practice to ensure re-use of common functionality, optimum use of key staff and best operational and cyber practice across the enterprise. This kind of standardization is happening across both technology platforms such as Public Website, Intranet Site, Document Management and also business lines such as Grants, Licensing, Mobile Inspection and Call Centers.

The following two enterprise level efforts highlight the collaboration efforts carried out by ITS with agencies.

NYS Public Website standardization: In October 2015, ITS held a conference highlighting the innovative New York State Agency Redesign initiative to communicate directly to agencies about the coming platform service offering to handle content management. For 2017, ITS is scheduling a follow up to the initial conference to reinforce the goals of the initiative and display current best practices in initial site launches, and provide a road map for future enhancements and innovations. ITS will also work with the DigitalNY team to create information and presentations in current best practices and roadmap of innovations for Agency meetings that are part of the web redesign process. Similar cross collaboration happens across agencies for both licensing and inspection functions, where the best practices extend beyond technology into business process standardization to offer NYS citizens and businesses a streamlined experience when working across agency boundaries.

Leveraging investments on Microsoft Office 365 platform: NYS' investment in Office 365 includes many features in addition to email. One of the key component is Sharepoint. Prior to ITS handful of agencies used this technology as a document sharing platform, and not everyone in the State had access to these tools. Agencies have used Sharepoint for several purposes including Intranet sites, project repositories, and simple workflow tools.

ITS formed the SharePoint Collaboratorium several years ago as an internal ITS group to ensure consistent, best practice deployment of SharePoint sites for ITS and the agencies it serves. ITS plans that the Collaboratorium resources and best practices will be available to agency users as well. To that end, ITS is creating a task force of Agency SharePoint users to share best practices and inform the ongoing design of the prototype agency intranet. ITS will leverage the task force to promote best practices for agency specific business needs and assess initiatives that all agencies will benefit from. One such example of best practice that ITS is planning to establish is adoption of NYS' investment to standardize SharePoint as the platform for agency intranet websites. ITS is currently creating a prototype Agency Intranet using SharePoint, leveraging input from agency users of SharePoint and the "SharePoint Collaboratorium."

The above are just few examples of how ITS is collaborating with agencies. To further promote the sharing of technology innovations across ITS which will in turn enable them to share those ideas with their agencies, ITS further plans to have the CTO office lead a community of practice ("COP") that includes Solutions Architects existing in the clusters. The purpose of these efforts is to coordinate information sharing on Agency use of ITS technology across the enterprise.

Additionally, on a day-to-day basis interaction occur at many levels within the agencies, including the leadership and management levels. Some of the roles within the ITS that are assigned specifically to each agency include:

Customer Relationship Manager (CRM): A senior leader within an ITS Cluster who is an Agency's primary interface with the ITS Organization – for services not managed by the Service Desk and for documented requests/incidents requiring escalation for resolution.

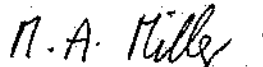
Service Delivery Manager (SDM): A senior delivery leader within ITS Operations who understands operational teams and provides a cross-functional viewpoint and response capability for a Cluster.

These two roles focus on the specific business needs for one or more agencies on a day to day basis, including service requests, attending to incidents and communicating root cause of critical incidents to agency executives and discussing improvement opportunities.

Overall, ITS has well defined functions and organizational units to work with state agencies to facilitate their sharing of successful and innovative practices to more efficiently and effectively manage ITS resources and assets. As with any area, ITS remains open to ideas and feedback from agencies, received through the day-to-day interactions with agencies, and incorporating best practices into our approach.

If you have any questions regarding this report, please do not hesitate to contact Rajni Chawla, ITS Director of Internal Audit, at (518) 457-5465.

Very truly yours,



Margaret Miller
NYS Chief Information Officer
Director, NYS Office of Information Technology Services

MAM/sb

cc: Governor Andrew M. Cuomo
Lt. Governor Kathleen C. Hochul
Senator John J. Flanagan
Senator Andrea Stewart-Cousins
Senator Catharine M. Young
Senator Liz Krueger
Assemblyman Carl E. Heastie
Assemblyman Joseph Morelle
Assemblyman Brian M. Kolb
Assemblyman Herman D. Farrell, Jr.
Assemblyman Bob Oaks
Assemblywoman Ellen Jaffee
Budget Division Director Robert Mujica