OBM | Office of Internal Audit

ASSURANCE MEMORANDUM

To: William Calderone, Chief Information Officer, Department of Youth Services

From: Cindy Klatt, Chief Audit Executive, OBM Office of Internal Audit (OIA)

Cc: Harvey J. Reed, Director, Department of Youth Services

Date: December 14, 2017

Subject: IT Governance Assurance Engagement

Background

The Ohio Department of Youth Services (DYS) is the juvenile justice agency for the state of Ohio. DYS is statutorily mandated to confine felony offenders, ages 10 to 21, who have been adjudicated and committed by one of Ohio's 88 county juvenile courts. Through DYS, youth are engaged in programming that is designed to address their criminological and behavioral needs. To fulfill its mission, DYS leverages IT within its governance and management approach. Recognizing a need to improve the collaborative efforts between business and IT functions, DYS requested OIA perform a review to assist the agency in assessing their IT Governance function.

During the audit, OIA identified opportunities for DYS to strengthen internal controls and improve business operations. A detailed listing of observations has been provided. This audit conforms to the International Standards for the Professional Practice of Internal Auditing. OIA would like to thank DYS staff and management for their cooperation and time in support of this audit.

This report is solely intended for the information and use of agency management and the State Audit Committee. It is not intended for anyone other than these specified parties.

Scope & Objectives

OIA staff was engaged to perform an assurance audit related to the agency's controls over IT Governance. The audit was performed between September 22, 2017 to December 5, 2017. The scope of this audit included reviewing the following components of IT governance: executive leadership and support, service delivery and measurement, IT organization and risk management.

The following summarizes the objectives of the review:

- Evaluate the design and controls related to IT Governance

Observations & Recommendations

The Observations and Recommendations include only those risks which were deemed high or moderate. If any low risk observations were made during the engagement, they were discussed with individual agency management and are not part of this report. There were no low risk observations for this engagement.

Objective	Conclusion*
Evaluate the design and controls related to IT Governance	**Improvement Needed***

*Refer to Appendix A for classification of audit conclusions.

Observation 1 – Inadequate Communication and Governance Structure

GTAG (Global Technology Audit Guide) guidance published by the Institute of Internal Auditors states that clear organizational structures, the operational nature of their components, how they communicate with each other, and accountability protocols are important for the IT function to enable the organization to achieve its objectives. Senior management should engage IT and the CIO in the strategic decisions about governance, enabling IT to add value in key decisions. The CIO should have access to the senior management team, and they should meet on a regular basis to discuss IT service delivery related to strategic goals.

During our review, OIA noted that the CIO is not periodically included in executive staff meetings with senior management to discuss strategic initiatives in DYS and their impact on IT and overall agency operations. Moreover, we also noted that DYS had not established certain processes regarding IT governance functions, such as periodic meetings on IT issues or oversight bodies such as an IT Governance Committee or IT Steering Committee within DYS' overall governance structure, which may inhibit communications and decision-making regarding IT projects within the business. On the divisional level, IT is starting a periodic meeting next month to discuss Business-IT projects.

The lack of IT governance functions and related communication, support and involvement of senior management with IT could result in unsound IT investments, IT misalignment with the business objectives, and inappropriate measuring of IT's performance.

Recommendation

DYS senior management should assess the functions and current communication structure with IT to provide the CIO with adequate access to senior management and knowledge regarding strategic initiatives in order for the CIO and IT to contribute to the success of the agency. Senior management should involve the CIO in strategic planning and related business processes of the agency by inviting the CIO to attend executive staff meetings and establishing periodic meetings and IT-related oversight bodies including an IT Governance and Steering Committees.

Management Response

DYS has been working, even prior to commencement of this OIA review, to address this issue. An IT governance process has been established both in policy and procedure. We are providing additional documentation that includes an approved agency policy and working documents associated with the governance process. Membership of the committee is comprised of the CIO (chair), the CFO, and the Assistant Director. The governance group will provide not only for project approval and prioritization, but will act as a strategic and process sounding board for agency IT direction. While still new in its application, we believe this structure will address the concerns noted above.

Additionally, the CIO will begin regularly occurring meetings with various groups of the agency to provide a forum to discuss strategic planning and related business processes. This will include both executive staff and other internal stakeholders across various functional areas.

Risk	Remediation Owner	Estimated Completion Date
Moderate	CIO	September 2018

Observation 2 – IT management is not using specific metrics to evaluate efficiency and value creation

GTAG indicates that a clear IT strategy, with appropriate performance indicators, is one of the keys to effective IT governance. Metrics and goals are established to help IT perform on a tactical basis and to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of organizational leaders.

During our review, we noted that there is no effective performance management framework with appropriate key performance indicators (KPIs) to enable proactive measurement and analysis of IT performance and the impact on achieving organizational goals.

Failure to measure operational and financial performance in IT can lead to operational and financial inefficiencies, inability to achieve operational and financial goals and lack of alignment with goals and strategic mission.

Recommendation

In a model, IT governance structure, the IT function is measured not just on its performance related to operational and tactical plans, but also on its impact on the achievement of organizational objectives documented in the strategic plan.

Metrics should be in place to measure the effectiveness of the day-to-day operational aspects of the IT function. From an operational perspective, IT management will require more technical metrics such as system uptime/downtime, helpdesk ticket open-to-closed ratio, peak usage time periods, capacity, and utilization. To enable easier measurement of IT's impact on the achievement of organizational goals, the agency could break down these goals into lower level operational component objectives and use various metrics such as service level agreements (SLAs) and operations level agreements (OLAs).

IT-related financial metrics also play an important role in measuring strategic, operational, and technical results. Outcomes enabled by IT should be measured to show the value contribution at the strategic levels (organizational plans, business-IT balanced scorecard, service level oversight) and tactical levels (multiple departmental IT balanced scorecard, project metrics, application systems metrics, service level agreements). These measurements allow IT management to understand how it is performing relative to the strategic plan, and to better understand how to more effectively manage the cost of IT service delivery.

Management Response

IT Management team will be evaluating various tools to the measure the effectiveness of operations, and will incorporate those with current stats being tracked. Additionally, we will review several models of the Balanced Scorecard and implement a modified version as fitting for our Agency.

Risk	Remediation Owner	Estimated Completion Date
Moderate	CIO	September 2018

Observation 3 – Lack of Formalized IT Governance Policy

GTAG indicates that formal controls such as documented policy and procedures are key controls that an organization should have in place to mitigate risks related to IT governance. GTAG also provides guidance that IT policies and procedures should be approved by the CIO or equivalent party that has final responsibility for these documents.

During our review, OIA noted that DYS had developed a draft IT Governance Policy that provides guidance for managing projects, DYS investment plan, and sustaining the DYS mission and business continuity plan. However, the policy has not been completed and approved by management. Also, OIA noted that the draft policy does not specifically define the requirement for the Information Technology Services Governance Group (ITSGG), established in the policy, to periodically report to executive management to ensure alignment with the organization strategic objective.

Lack of a formally documented IT Governance Policy can lead to misalignment between IT and business objectives, inefficient use of IT resources, and unsound IT investment decisions.

Recommendation

Management should continue to finalize and approve the DYS IT Governance Policy and distribute the approved policy to the appropriate stakeholders. DYS should maintain evidence of the approval and distribution of the policy for an agency approved duration.

Management should update the IT Governance Policy to address the following items:

- Reporting to executive management
- IT governance committee review of IT policies and procedures on a periodic basis
- Regular IT governance committee meetings are conducted

Management Response

DYS has been working, even prior to commencement of this OIA review, to address this issue. An IT governance process has been established both in policy and procedure. The attached documentation includes an approved agency policy and working documents associated with the governance process. Membership of the committee is comprised of the CIO (chair), the CFO, and the Assistant Director. The governance group will provide not only for project approval and prioritization, but will act as a strategic and process sounding board for agency IT direction. While still new in its application, we believe this structure will address the concerns noted above.

Additionally, the CIO will begin regularly occurring meetings with various groups of the agency to provide a forum to discuss strategic planning and related business processes. This will include both executive staff and other internal stakeholders across various functional areas.

Risk	Remediation Owner	Estimated Completion Date
Moderate	CIO	February 2018

Observation 4 – Lack of Formal Risk Management Framework

GTAG indicates risk management is a key component of an effective IT governance structure within an organization. IT governance helps ensure close linkage to an organization's risk management activities and includes processes and combinations of controls that help organizations balance their overall IT risk profile and organizational objectives within risk appetite and tolerance.

During our review, we noted that project management level risk and cost analysis are considered by the IT Project Administrator for IT project selection. However, DYS has not adopted a risk management framework or developed formal documentation which describes the identification and assessment of IT risks within the Agency.

Lack of an appropriate risk management framework in place may lead to improper identification of vulnerabilities to data and infrastructure, improper mitigation of risks, and misalignment of key internal controls.

Recommendation

Management should develop formal documentation that describes the identification and assessment of IT risks within DYS. This documentation should include but not be limited to a description of what is meant by risk and risk management in DYS, a definition of risk tolerance and a description of how DYS applies the definition, a statement on the willingness to accept risk, and a determination of how risk acceptance should be defined in terms of trade-offs against objectives.

The agency should develop a risk management program where risk management practices do not exceed the enterprise risk appetite/tolerance. Moreover, management should develop and monitor risk management processes that identify, track, measure, prioritize, and report issues for remediation/implementation through a Risk Action Plan. For guidance, management may review various frameworks such as the ISACA Risk IT methodology to develop DYS risk management practices.

Management Response

DYS has been working, even prior to commencement of this OIA review, to address this issue. An IT governance process has been established both in policy and procedure. The attached documentation includes an approved agency policy and working documents associated with the governance process. Membership of the committee is comprised of the CIO (chair), the CFO, and the Assistant Director. The governance group will provide not only for project approval and prioritization, but will act as a strategic and process sounding board for agency IT direction. While still new in its application, we believe this structure will address the concerns noted above.

Additionally, the CIO will begin regularly occurring meetings with various groups of the agency to provide a forum to discuss strategic planning and related business processes. This will include both executive staff and other internal stakeholders across various functional areas.

IT Services does do risk management for every project and assignment, but does not have a formalized process for documenting and sharing this information. We plan to establish a program which will help us to track and mitigate what is done and how often.

Risk	Remediation Owner	Estimated Completion Date
Moderate	CIO	May 2018

Observation 5 – Lack of Compliance Monitoring and Reporting

GTAG indicates that the organization's senior management governance group should ensure compliance with external regulatory governance issues that may impact the organization.

During our review, OIA noted that formally documented procedures for compliance monitoring and reporting to a senior management group is not in place.

Lack of timely communication of compliance and regulatory issues to stakeholders may lead to misalignment between IT-related objectives and strategies and external legal or regulatory requirements.

Recommendation

As part of a risk management framework, the Information Technology Services Governance Group (ITSGG) identified in the draft DYS IT Governance Policy should develop a communication strategy with stakeholders whereby all parties involved can stay abreast of compliance and regulatory governance issues. This should include stakeholders informing ITSGG of mandatory reporting requirements. Compliance and regulatory issues can include data classification, contractual obligations, emerging trends/issues, and periodic policy review of DYS policy and whether policies and procedures align with state and federal policy changes.

Management Response

DYS has been working, even prior to commencement of this OIA review, to address this issue. An IT governance process has been established both in policy and procedure. The attached documentation includes an approved agency policy and working documents associated with the governance process. Membership of the committee is comprised of the CIO (chair), the CFO, and the Assistant Director. The governance group will provide not only for project approval and prioritization, but will act as a strategic and process sounding board for agency IT direction. While still new in its application, we believe this structure will address the concerns noted above.

Additionally, the CIO will begin regularly occurring meetings with various groups of the agency to provide a forum to discuss strategic planning and related business processes. This will include both executive staff and other internal stakeholders across various functional areas.

IT Services will review ways to; ensure compliance with DAS, communicate compliance with stakeholders, review metrics & reports on compliance, comprise a list of what is tracked and who is responsible, and document audit requirements.

Risk	Remediation Owner	Estimated Completion Date
Moderate	CIO	June 2018

Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the observations and recommendations suggested above. However, these observations reflect our continuing desire to assist your department in achieving improvements in internal controls, compliance, and operational efficiencies.

*Refer to Appendix A for classification of audit observations.

Appendix A – Classification of Conclusions and Observations

Classification of Audit Objective Conclusions

Conclusion	Description of Factors
Well-Controlled	The processes are appropriately designed and/or are operating effectively to manage risks. Control issues may exist, but are minor.
Well-Controlled with Improvement Needed	The processes have design or operating effectiveness deficiencies but do not compromise achievement of important control objectives.
Improvement Needed	Weaknesses are present that compromise achievement of one or more control objectives but do not prevent the process from achieving its overall purpose. While important weaknesses exist, their impact is not widespread.
Major Improvement Needed	Weaknesses are present that could potentially compromise achievement of its overall purpose. The impact of weaknesses on management of risks is widespread due to the number or nature of the weaknesses.

Classification of Audit Observations

Rating	Description of Factors	Reporting Level
Low	Observation poses relatively minor exposure to an agency under review. Represents a process improvement opportunity.	Agency Management; State Audit Committee (Not reported)
Moderate	Observation has moderate impact to the agency. Exposure may be significant to unit within an agency, but not to the agency as a whole. Compensating controls may exist but are not operating as designed. Requires near-term agency attention.	Agency Management and State Audit Committee
High	Observation has broad (state or agency wide) impact and possible or existing material exposure requiring immediate agency attention and remediation.	Agency Management and State Audit Committee