DEPARTMENT OF
ADMINISTRATION

OFFICE OF MANAGEMENT & BUDGET

Office of Internal Audit

One Capitol Hill
Providence, RI 02908-5890

Office: (401) 574-8170
Fax: (401) 574-9255

April 23, 2025

Governor Daniel J. McKee
Office of the Governor
82 Smith Street
Providence, RI 02903

Dear Governor McKee:

The Office of Internal Audit (OIA) has completed its annual collection of responses from state agencies and quasi-agencies, as mandated by Rhode Island General Laws § 35-14-6, Financial Integrity and Accountability Act (FIAA). The FIAA reporting process is a statewide self-assessment of the adequacy of internal controls.

Enclosed is our report of the 2024 responses received from 80 respondents, comprising state departments, agencies and quasi-agencies. Developed by OIA, this questionnaire encompasses strategic and general operations, financial information, human resource management, regulatory compliance, internal controls, information technology controls and government service. It featured both yes/no and Likert scale-rated questions. Additionally, the respondents had the opportunity to provide further written commentary.

OIA has developed a new scoring methodology to assess risk based on their responses. The report highlights both areas of success and risk areas identified across agencies.

Respectfully,

Andrew Manca

Digitally signed by Andrew Manca
Date: 2025.04.23 13:41:23 -04'00'

Andrew Manca
Chief, Office of Internal Audit

Cc: Internal Audit Advisory Group
The Honorable Marvin L. Abney, Chairman, House Committee on Finance
The Honorable Louis P. DiPalma, Chairman, Senate Committee on Finance
Sharon Reynolds Ferland, House Fiscal Advisor
Steven Whitney, Senate Fiscal Advisor

Contents

Introduction 3
Background 3
Methodology 5
Results and Insights 5
Risk Category Breakdown and Rationale for Selection 5
Statewide Risk Assessment Overview 9
Survey Section Analysis 10
Areas of Strength 11
Identified Risk Areas 13
Proposed Actions and Audit Plan Updates 16

April 23, 2025

Introduction

The Office of Internal Audit (OIA) distributed a statewide self-assessment questionnaire of internal controls to 80 possible respondents which include state departments, agencies and quasi-public agencies as part of the Financial Integrity and Accountability Act (FIAA) reporting process. OIA designed the questionnaire to evaluate the effectiveness of accounting and administrative controls across state agencies and quasi-public corporations in Rhode Island. The goal of the questionnaire is to provide clarity and consistency of the information reported, as well as to ensure an efficient process for identifying and addressing risk. OIA revamped the risk assessment methodology used in the 2024 questionnaire, categorizing survey segments according to specific risk areas. By introducing standardized scoring, including the use of a Likert scale (i.e., “strongly agree” to “strongly disagree”) for responses, OIA aims to provide a more objective and reliable basis for assessing risk and informing future audit planning.

Presented below is an overview of the background on the FIAA questionnaire, detailing the changes made to the FIAA reporting process, the rationale behind those changes, the methodology employed, as well as the questionnaire results and analysis pertinent to the completed reporting process.

Background

In 1986, the General Assembly enacted Rhode Island General Laws (RIGL) § 35-14, known as the Financial Integrity and Accountability Act.[1] The statute mandates that heads of state agencies establish systems of internal accounting and administrative controls and submit a report on the adequacy of those controls by the end of each calendar year.[2] The report, which must be signed by the agency head and addressed to the Governor, serves as a critical component of the state’s internal oversight. In 1995, the General Assembly expanded the scope of these requirements to quasi-public corporations through the enactment of RIGL § 35-20, entitled Public Corporation Financial Integrity and Accountability. This law applies the same internal control requirements to quasi-public corporations as it does to state agencies.[3]

[1] webserver.rilegislature.gov/Statutes/TITLE35/35-14/35-14-2.htm
[2] webserver.rilegislature.gov/Statutes/TITLE35/35-14/35-14-6.htm
[3] webserver.rilegislature.gov/Statutes/TITLE35/35-20/35-20-2.htm

In 2006, OIA reshaped the FIAA reporting process to enhance the efficiency of the process and provide a more streamlined method for agencies and public corporations to report on their systems of internal accounting and administrative controls. OIA developed a questionnaire, segmented into various categories, including, but not limited to: General Information, Strategic, Internal Controls, Human Resource Management, Regulatory Compliance and Government Service. The questionnaire results are due from respondents by mid-January, allowing them sufficient time to compile and verify data as of December 31, ensuring accuracy and reflection of year-end information. The survey has been updated and revised several times over the years.

In 2024, OIA undertook a significant revision of the questionnaire, with the primary aim to improve the assessment of residual risk and utilize the results from the questionnaire to inform the development of the audit plan for the following fiscal year. While the previous version of the questionnaire satisfied the statutory requirements, OIA explored opportunities for enhancing consistency in response options, which would help make the assessment of residual risk more objective and streamlined. OIA's first step in improving the process was to review the current questionnaire segments and assign risk categories to each. These risk categories include Operational, Strategic, Legal, Talent and other relevant classifications. Risk assignment enables the precise categorization of potential threats within each segment. This approach allows for a more targeted risk mitigation strategy and enhances the overall effectiveness of identifying areas that may require further auditing in subsequent audit plans.

Each risk category is carefully defined based on the specific questionnaire segment to which it relates. For example, the "Internal Controls" segment is classified under operational risk, focusing on concerns that could arise within an agency's processes, personnel, systems or external environment, all of which could potentially affect the agency's operational efficiency, integrity and continuity. The internal control policies and procedures in place should effectively mitigate operational risks by ensuring the detection, prevention and correction of any identified issues.

After categorizing the segments, OIA revised most of the survey's questions, transforming them into Likert-scale rating questions. This allows respondents to select answers from a linear set of responses that range from low to high. The transition to a standardized rating scale has enabled consistent and objective scoring based on respondent answers, improving the comparability of results across agencies. Furthermore, open-ended questions are retained for each questionnaire segment to allow respondents to provide additional insights or context not captured by the quantitative responses.

Lastly, OIA implemented a risk assessment scoring framework to track and analyze the responses from the 80 respondents. This framework facilitates the tracking of internal responses and provides OIA with the ability to analyze the results across all respondents. By comparing responses, OIA gains a better understanding of how agency leadership perceives their internal controls and can compare them to the broader state response. This comparative analysis aids in identifying areas of concern and informs the development of the audit plan.

Methodology

To address the statute's mandated objectives, OIA:

- Administered the questionnaire to meet the requirements outlined in Rhode Island General Laws § 35-14-2 to ensure that all state agencies provide the necessary data for OIA's review and subsequent reporting.
- Tracked participation to ensure a high response rate and to identify any non-responses or incomplete submissions. For those agencies identified as non-respondents, OIA conducted follow-up outreach to encourage and facilitate submission.
- Aggregated and analyzed the self-assessment data to identify common risk trends, strengths and weaknesses across the various state agencies.

Results and Insights

The following sections provide a summary of self-assessment responses collected from 80 respondents. The internal control assessment data was analyzed using the risk assessment scoring framework. This analysis highlights the insights related to the effectiveness of the internal controls across different agencies offering an understanding of the identified risks.

Risk Category Breakdown and Rationale for Selection

To evaluate potential risks, the questionnaire categorizes risks into distinct questionnaire segments, each representing a specific area of focus. Each segment is associated with its own set of characteristics that help categorize the risks effectively. These categories were selected to address the key areas that influence an agency's ability to achieve its objectives, maintain operational efficiency and meet compliance requirements. Below is a breakdown of each of the five categories, their corresponding segments and a brief description of the risk associated with each segment.

1. Legal & Compliance Risks

Grants

Risk Description: The risk of damage to an agency's standing, credibility and public perception regarding its relationships with constituents and funding, especially related to federal funds compliance and ongoing regulatory investigations.

Rationale: Legal and compliance risks are especially critical in areas where an agency manages grants and federal funding. Failure to comply with reporting requirements or regulations could lead to reputational damage and loss of funding. By categorizing this risk separately, the agency can focus on maintaining legal and regulatory compliance.

2. Operational Risks

Capital Assets

Risk Description: The risk that arises from an agency's ability to effectively manage capital assets, including acquisition, maintenance and disposal.

Rationale: Capital assets are a significant portion of an agency's resources. Poor management of these assets can lead to financial inefficiencies and missed opportunities for cost savings.

Health & Safety

Risk Description: The risk that arises from operational processes, employees, or systems, which impacts both employees and the public. It includes potential disruptions in service due to health and safety concerns.

Rationale: Health and safety concerns have both operational and legal implications. Protecting employees from risks ensures the agency remains compliant with regulations and minimizes operational disruptions. These risks directly impact the agency's ability to provide consistent services to constituents.

Information & Communication

Risk Description: The risk that arises within an agency's processes, employees, systems, or external environment, impacting its efficiency, integrity and continuity.

Rationale: Effective communication and efficient processes are vital to the smooth operation of any agency. Miscommunication or broken processes can create inefficiencies or lead to incorrect decisions. By identifying operational risks, agencies can implement business operations plans, training and communication strategies that help mitigate these risks.

Information Technology Controls

Risk Description: The risk related to failures in IT systems and the handling of sensitive data that affect the agency's efficiency, integrity and continuity.

Rationale: In today's digital age, effective IT controls are necessary to protect sensitive information and maintain operational continuity. This category assesses whether the agency has the right IT policies and procedures to prevent or address potential risks related to information security and system integrity.

Internal Controls

Risk Description: The risk associated with failures in internal processes, employees, or systems, which affects the agency's ability to detect, prevent, or correct operational issues.

Rationale: Strong internal controls are fundamental for ensuring that an agency operates efficiently and within legal boundaries. Proper internal controls prevent fraud, errors and inefficiencies from occurring, while also enabling the agency to quickly address any operational issues.

3. Regulatory Risks

Regulatory

Risk Description: The risk of damage to an agency's standing, credibility and public perception due to failure to comply with relevant regulations. This includes the risk of losing trust from constituents and stakeholders.

Rationale: Regulatory compliance is foundational for any agency. It ensures that the agency's policies and procedures are in line with applicable legislation and that constituents are adhering to those policies. Failing to maintain compliance could result in significant legal and reputational consequences.

4. Strategic Risks

Government Services

Risk Description: The risks related to an agency's procedures for collecting information about the demographics it serves and the quality of the services it provides.

Rationale: Agencies need effective mechanisms for gathering and analyzing data on the demographics they serve. This information helps them adjust policies and improve service delivery, mitigating potential strategic risks. Without such procedures, agencies risk misaligning their services with public needs.

Strategic Information

Risk Description: The risks faced by an agency in achieving its long-term objectives, stemming from factors such as population within the state and political dynamics, as well as poor strategic planning processes.

Rationale: An agency's ability to successfully implement long-term objectives hinges on comprehensive strategic planning. The risks in this area are often difficult to foresee but can have a significant impact on the agency's direction and success. Identifying these risks allows agencies to better allocate resources and avoid potential setbacks.

5. Talent Risks

Human Resource Management

Risk Description: The risk associated with effectively managing and optimizing human resources to support the agency's objectives.

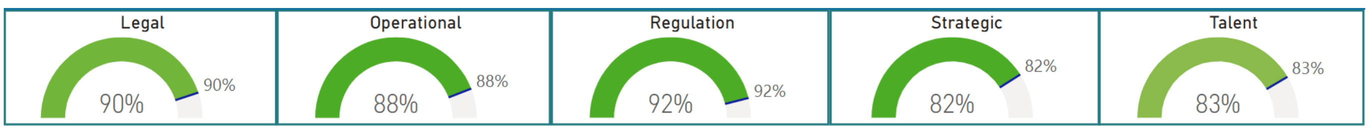
Rationale: Effective human resource management is essential for ensuring that the agency can recruit, train and retain qualified personnel to meet its mission. This category addresses the risks that arise from ineffective management of human capital, which could impact both short-term performance and long-term sustainability.

The categories selected for the risk assessment reflect the key areas that are essential for an agency's operations, compliance and overall effectiveness. By evaluating each category, the agency can assist OIA in pinpointing vulnerabilities that may affect each agency's long-term objectives, operational efficiency, or legal standing. This structured approach allows for a comprehensive view of an agency's current risk profile, enabling targeted mitigation strategies and improvement efforts.

Statewide Risk Assessment Overview

The results of the questionnaire provide insight into the state's overall risk management landscape. To facilitate an understanding of the findings, the statewide results are categorized according to the identified risk segments. These categories reflect the key areas in which agencies are assessing and managing their risks when they completed the self-assessment questionnaire. The scores are expressed as a percentage of the highest possible score; therefore, a lower score would indicate greater risk, and a higher score would represent less risk. It is important to consider how agencies are performing across these categories as whole, as each one plays a crucial role in shaping the state's outcome.

Figure 1: Statewide Risk Assessment – Full Survey Results by Category



Overall, more than 80% of respondents indicated a high level of consensus and confidence in the existing controls and processes, as seen in Figure 1, which reports aggregate risk assessment results by category. The self-assessment indicates that Regulation is perceived as the area with the least amount of risk. This category shows that for 2024 agencies felt confident in their ability to access grant opportunities that support funding for initiatives. Additionally, agencies reported strong performance in tracking and meeting grant compliance requirements. However, there are notable areas for improvement, particularly within the Strategic Risk category. As a whole, the state scored the lowest in this area, with an overall score of 82%. Agencies expressed concerns over factors that could impact their long-term objectives, including budget cuts and funding uncertainties, which are seen as significant threats to their operational capacity.

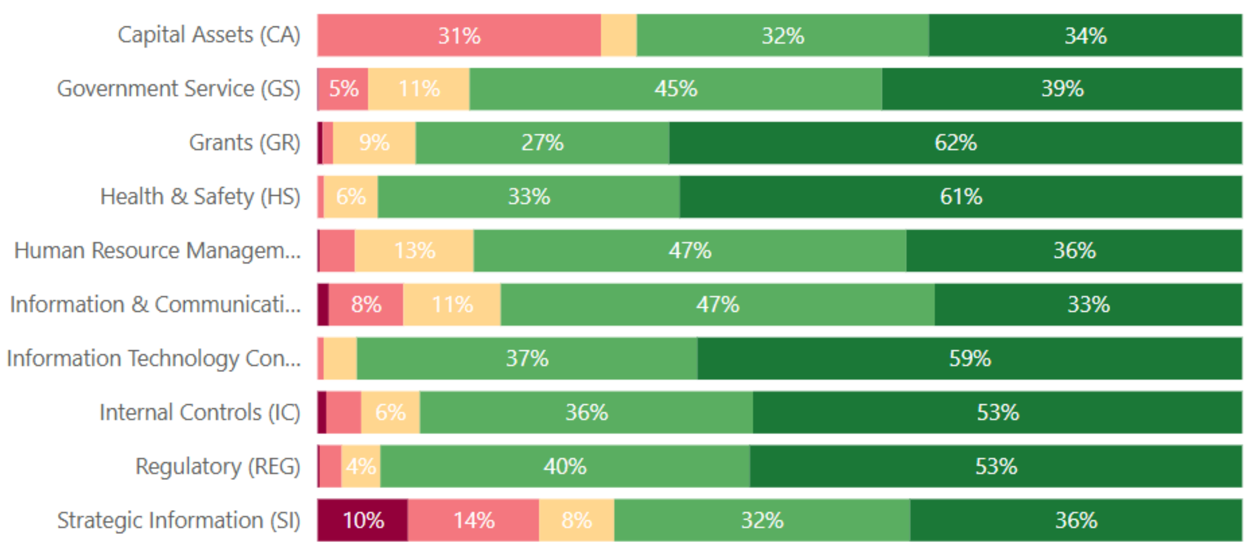
While the state's performance in Strategic Risk is relatively higher compared to other areas, the main concerns stem from external factors beyond the agencies' control. These factors include potential legislative changes, demographic shifts and, as previously mentioned, budget cuts. These external challenges were cited as key sources of risk that may impede the state's ability to effectively plan and implement long-term strategies.

Though the state has demonstrated strengths in regulatory and operational areas, addressing the strategic risks identified is necessary for improving the overall resilience and effectiveness of state agencies. The following provides a deeper analysis of the specific survey results, highlighting both areas of success and those requiring further attention.

Survey Section Analysis

OIA took a closer look to identify any areas that may have scored higher in risk than others. To gain a more detailed understanding, OIA analyzed the risk scores by segment of the FIAA questionnaire, as shown in the Figure 2 below. The scoring results are primarily based on a Likert scale, where 'Strongly Disagree' (indicated by dark red) represents higher risk, and 'Strongly Agree' (indicated by dark green) reflects lower risk. This approach allows for a more targeted examination of specific risk factors and highlights areas that may require additional focus or improvement.

Figure 2: Statewide Risk Assessment – Full Survey Results by Segment



The Capital Assets segment draws immediate attention due to its risk score of 31%, which corresponds to the darkest red on the Likert scale. This score represents the highest percentage of respondents who selected 'Strongly Disagree' indicating a higher perceived risk within this segment compared to the others. Capital assets represent a significant portion of public resources and require effective management to ensure proper maintenance, cost-efficiency and long-term sustainability. A high percentage in this category could signify potential vulnerabilities in the management and oversight of these assets, which could lead to inefficiencies, safety concerns, or unanticipated costs.

In response, OIA reached out proactively to the Division of Capital Asset Management and Maintenance (DCAMM) and provided them with a list of agencies expressing concerns in this area. DCAMM is responsible for managing and maintaining an asset portfolio of 1,800 buildings statewide, ensuring they meet the highest standards for health, safety, security, accessibility, energy efficiency and comfort for state employees and the public they serve. Providing DCAMM the list of agencies that expressed concern allows the division to engage with these agencies and discuss their specific challenges as well as potential risk mitigation strategies.

OIA took a similar approach for other questionnaire segments that indicated any level of risk, regardless of the score. For example, OIA shared the list of agencies with human resource management concerns with the Division of Human Resources, which oversees strategic planning, personnel administration, labor relations, employee benefits, training, development and disability management for state employees. Agencies that scored higher risk in the Information Technology (IT) segment were referred to the Department of Administration’s Enterprise Technology Strategy and Services division, which manages the state's information technology resources. This approach ensured that even if an agency was not selected for inclusion in next year’s audit plan, they were still provided the opportunity to take proactive steps toward addressing their concerns by engaging with relevant personnel.

Areas of Strength

Upon analyzing the FIAA survey results, certain risk areas were identified as strengths within the state agencies, with IT and Grants standing out as areas of high performance. Though Grants ranked as one of the lowest in risk, it is important to understand why this area was ultimately deemed a strength. State agencies have effectively developed processes for managing grant applications, mitigating risks related to federal and state funding and ensuring compliance with reporting requirements. Agencies also demonstrated a clear understanding of the importance of transparency and accountability in utilizing grant funds, which contributed to the positive performance in this area. The consistency and strength of the procedures in place are also contributing factors to the low-risk scores reported.

Despite the growing complexity of cyber threats and the increased reliance on technology to manage sensitive data and operations, agencies responded with a shared confidence in their IT infrastructure. Many stated that they have procedures in place to address any potential security breaches. This includes a clear process for responding to cybersecurity incidents, ensuring that breaches are quickly identified, reported and mitigated in accordance with best practices.

ETSS's proactive approach to cybersecurity and data protection is a key factor in the low-risk score. Agencies expressed confidence in their password management protocols, ensuring that all employees adhere to strict password policies that prevent unauthorized access to critical data. By continuously updating and enforcing these policies and procedures, state agencies are actively minimizing the risk of security vulnerabilities. Additionally, these updates are regularly communicated across all agency levels to ensure consistent implementation and compliance. This culture of security awareness across departments is a driver in maintaining a high level of protection for both sensitive data and agency operations. Many agencies expressed confidence in their regular training and simulations, such as simulated phishing emails, to ensure employees are well-equipped to recognize potential security threats and respond appropriately, further reducing the likelihood of security gaps.

The State's approach to Information and Communication was another standout with a score of 80%. Agencies recognize the vital role of effective communication in maintaining operational integrity and transparency. Agencies have demonstrated that clear communication channels and well-defined processes are essential for both managing day-to-day operations and ensuring compliance with regulatory requirements. This focus on communication enhances overall operational efficiency, mitigates risk and fosters stronger relationships between agencies and the public.

The scores in Grants, Information Technology and Information and Communication highlight the state's proactive and strategic approach in managing risks. By maintaining strong internal policies, ensuring consistent employee training and fostering a culture of compliance and security, the state is well-positioned to mitigate risks in these key areas. Furthermore, these strengths serve as examples of best practices for other areas within state agencies to emulate, ensuring ongoing improvement in risk management.

Identified Risk Areas

Although every questionnaire segment is important, from a performance audit perspective, OIA is primarily focusing on operational and strategic questionnaire segments, such as Internal Controls and Strategic Information.

Strong internal controls are fundamental to ensuring the accuracy and reliability of an agency's operations, financial reporting and compliance with laws and regulations. Without adequate controls in place, agencies risk potential errors, fraud and mismanagement, which can lead to financial losses, legal consequences and a loss of public trust. Agencies expressed particular concern in Internal Controls around adequate staffing and existing financial resources. If the agency lacks adequate staffing, they may be unable to ensure that all control activities are in place and operating as designed, thus increasing the likelihood of gaps or weaknesses in control procedures. This could compromise the effectiveness of the agency's operations.

The Strategic Risk category scored the highest risk level statewide, indicating a higher perceived risk. The Strategic Information questionnaire segment within the Strategic Risk category received a score of 24%, ranking it as the second-highest perceived risk category among the questionnaire segments. The questions posed to agencies ranged from strategic planning processes to SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis, focusing on how agencies assess their strategic position and plan for the future. Like the Internal Controls section, agencies expressed significant concerns over budget cuts, funding uncertainties, proposed legislative changes and demographic shifts, all of which are factors that can significantly disrupt an agency's long-term objectives.

Budget cuts and funding uncertainties may limit an agency's ability to maintain its core services and operations, leading to potential reductions in staffing, delayed projects or cutbacks in essential programs. When agencies do not have a clear understanding of their financial outlook, it becomes difficult to set realistic strategic goals or allocate resources effectively. Furthermore, the agency may struggle with long-range planning or respond to emerging needs within their communities, ultimately putting them at a disadvantage in meeting their objectives.

Legislative changes can also have a considerable effect on strategic planning. Legislative reforms often lead to changes in regulations, mandates, or compliance requirements, which can divert resources and attention away from an agency's established objectives. Agencies must continuously adapt to these changes, often needing to reallocate budgets, modify their strategies, or adjust their operational goals to remain in compliance. This can redirect valuable resources away from long-term planning and strategic initiatives execution.

Finally, demographic shifts (such as population changes, aging populations, or changes in workforce composition) are also noteworthy factors for many agencies. These shifts can affect demand for services, create new challenges and require agencies to re-evaluate their service delivery models. For example, if an agency's primary focus is on healthcare or social services, an aging population could place an increased strain on resources and necessitate changes to the agency's operations, staffing levels and long-term planning.

Each of these factors present challenges to agencies, underscoring the importance of robust and flexible strategic planning that can anticipate and adapt to both internal and external influences. These concerns highlight the complexity of strategic risk management and the need for agencies to have a well-defined and adaptive approach to meet the demands of an ever-changing environment.

The Operational Risk category, which encompasses aspects such as internal controls, staffing and resources, is another area of concern for some agencies. As previously mentioned, concerns related to adequate staffing levels are prevalent, particularly when agencies recognize that a lack of sufficient personnel can hinder the effective implementation of internal controls. These internal controls are designed to ensure that agency operations run efficiently, securely and in compliance with applicable regulations. When internal controls are not consistently applied or monitored due to staffing shortages, agencies risk overlooking potential inefficiencies, fraud, or errors, which over time can result in greater vulnerabilities.

Furthermore, agencies expressed concerns regarding the adequacy of their existing financial resources, technologies and equipment. These resources support the day-to-day operations of an agency and ensure that it can meet its objectives. If agencies are not equipped with the necessary tools or funding to perform their tasks efficiently, it impacts their ability to deliver services, meet regulatory requirements and achieve strategic goals. For example, outdated or underfunded technology may not adequately support the constantly evolving requirements for data management, security, or communication efforts, increasing the risk of operational failure or breach.

Another area highlighted by agencies in Operational Risk is the lack of comprehensive written policies and procedures to guide operational activities, particularly those related to segregation of duties, independent checks and oversight. Segregation of duties is a fundamental principle of internal control, designed to prevent any one employee from having too much control over a process, thereby reducing the risk of errors or fraud. Without clearly defined policies in place, there is the potential for inadequate oversight, which can result in unauthorized or improper actions going undetected. The absence of effective checks and balances in operational processes can create an environment where control activities are not fully effective in safeguarding agency resources and achieving desired outcomes.

Concerns regarding staffing, resources and internal control procedures are not only reasonable but also important to address to manage operational risks within state agencies. Addressing these gaps and ensuring agencies are properly resourced and have strong, clear policies in place will mitigate the risk of operational inefficiencies, fraud and other compliance issues that could undermine their ability to meet their objectives.

The risks identified in both the operational and strategic segments provide valuable insights that will help guide the structure of OIA's audit plan for FY 2026. These risk areas — such as staffing shortages, resource limitations and inadequate internal controls — highlight key vulnerabilities within state agencies that require closer attention. By focusing on these areas in future audits, OIA can assist agencies in addressing the root causes of these risks and implementing effective solutions to improve their overall performance. Identifying and addressing these challenges proactively can also strengthen agencies' ability to meet their long-term goals and mitigate potential operational disruptions. Moving forward, these findings will inform the prioritization of agencies and risk areas for inclusion in the upcoming audit plan, ensuring that OIA's efforts align with the most pressing needs and opportunities for improvement across the state.

Proposed Actions and Audit Plan Updates

Under the Quasi-Public Corporations Accountability and Transparency Act (RIGL § 42-155-7), OIA is required to conduct an audit of each quasi-public corporation at least once every five years.[4] To comply with this mandate, OIA keeps an up-to-date audit schedule for the quasi-public agencies over for the next five years. The required and mandated audits, which includes the annual FIAA questionnaire, is outlined below. These upcoming audits were scheduled prior to incorporating the results of this year's FIAA questionnaire:

FY 2026 - Required & Mandated Audits	
Agency Name	**Estimated Completion Date**
Rhode Island Public Transit Authority	Quarter 1
Rhode Island Airport Corporation	Quarter 1
FIAA FY 2026 Questionnaire	Quarter 4

With the FIAA questionnaire results now received and reviewed, OIA proposes including additional agencies to the audit plan for the upcoming fiscal year. In addition to the FIAA results, OIA used other criteria to evaluate risk factors when selecting agencies to include in the FY 2026 audit plan, including:

- Increases and decreases in funding from the FY 2025 budget and proposed FY 2026 budget,
- An evaluation of agency financial discipline through comparison of budgeted funds to actual expenditures, and
- An evaluation of relative agency size through a comparison of budgeted funds.

Based on the FIAA survey results and other risk factors, OIA proposes including the following agencies in the FY 2026 audit plan.

[4] webserver.rilegislature.gov/Statutes/TITLE42/42-155/42-155-7.htm

FY 2026 Audit Plan	
Agency Name	**Estimated Completion Date**
Rhode Island Department of Motor Vehicles	Quarter 2
Rhode Island Department of Education	Quarter 3
University of Rhode Island	Quarter 3
Office of Health and Human Services	Quarter 3
Department of Transportation	Quarter 3
Department of Housing	Quarter 4
Behavioral Healthcare, Developmental Disabilities Hospitals	Quarter 4

It is important to note that this remains a proposed audit plan and is not yet final. Additionally, OIA receives recommendations from the Audit Advisory Group (AAG) regarding agencies to be considered for potential audits. The proposed plan will be reviewed with the AAG during the Q3 meeting and finalized for implementation in FY 2026.

If resources allow, OIA would also like to consider the following additional agencies for the inclusion in the audit plan. However, if these additional audits cannot be addressed in FY 2026, they may still be considered for FY 2027 depending on survey results. The next FIAA questionnaire will inform the planning process to ensure the audit plan remains aligned with the most current issues and risks.

FY 2026 – Additional Audit Plan Considerations
Agency Name
Department of Human Services
Department of Labor and Training