



OFFICE OF MANAGEMENT & BUDGET

Office of Internal Audit and Program Integrity

One Capitol Hill
Providence, RI 02908-5890

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

April 29, 2026

The Honorable Daniel J. McKee
Governor
Rhode Island State House
82 Smith Street
Providence, RI 02903

Dear Governor McKee:

The Office of Internal Audit and Program Integrity (OIAPI) has completed its annual collection of responses from state agencies and quasi-public 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 2025 responses received from 79 respondents, comprising state departments, agencies and quasi-public agencies. Developed by OIAPI, 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.

OIAPI developed a 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
Chief of Internal Audit and Program Integrity

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

Contents

- Introduction 3
- Background 3
- Methodology..... 4
- Results and Insights 5
 - Risk Category Breakdown and Rationale for Selection..... 5
 - Statewide Risk Assessment Overview 6
 - Survey Section Analysis 7
 - Areas of Strength 9
 - Identified Risk Areas.....10
- Proposed Actions and Audit Plan Updates.....13

Introduction

The Office of Internal Audit and Program Integrity (OIAPI) distributed a statewide internal controls self-assessment questionnaire to 79 possible respondents which included state departments, agencies and quasi-public agencies as part of the Financial Integrity and Accountability Act (FIAA) reporting process. OIAPI designed the questionnaire to evaluate the effectiveness of accounting and administrative controls across State agencies and quasi-public agencies 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.

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 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

OIAPI developed a questionnaire, with five risk categories that are 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 agency respondents on December 31, 2025, to reflect

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

year-end information. OIAPI uses the questionnaire to improve the assessment of residual risk and utilizes the results from the questionnaire to inform the development of the audit plan for the following fiscal year.

OIAPI implemented a structured risk assessment scoring framework to analyze responses across agencies. This framework enables comparative analysis, identifies emerging areas of concern, and strengthens that data-driven development of the audit plan. In 2025, OIAPI expanded the questionnaire to include a new section addressing the use and governance of Artificial Intelligence (AI). As AI tools become increasingly accessible and possibility of integration into agency operations, OIAPI determined it was important to proactively assess both adoption and risk management practices associated with these technologies.

The AI section evaluates whether agencies are utilizing AI in their processes or systems and assesses the maturity of related governance structures. Questions address strategic oversight, defined roles, and responsibilities, documentation of AI tools, pre-implementation risk evaluations (including data privacy, bias, and security considerations), compliance with confidentiality requirements, employee awareness of appropriate data use, and independent review of AI-generated outputs. By incorporating AI into the risk assessment framework, OIAPI can better understand how emerging technologies may influence operational, legal and strategic risks across agencies. This addition supports audit planning and helps ensure that evolving technological risks are appropriately considered in future audit coverage.

Methodology

To address the statute's mandated objectives, OIAPI:

- Administered the questionnaire to meet the requirements outlined in RIGL § 35-14-2 to ensure that all state agencies provide the necessary data for OIAPI'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, OIAPI conducted follow-up outreach to encourage and facilitate submission.
- Aggregated and analyzed the self-assessment data to conduct a risk assessment, and identify common risk trends, strengths and weaknesses across state and quasi-public agencies.

Results and Insights

The following sections provide a summary of self-assessment responses collected from 79 state and quasi-public agency 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 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 areas that influence an agency’s ability to achieve its objectives, maintain operational efficiency and meet compliance requirements. Below in Figure 1 is a breakdown of five categories, their corresponding segments, and brief risk descriptions.

Figure 1: Risk Assessment Framework and Categories

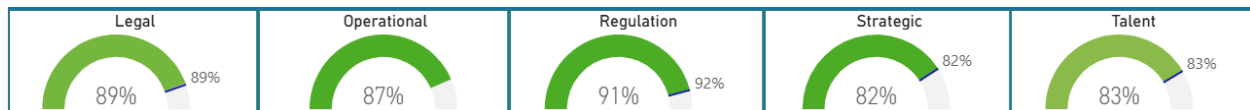
Risk Category	Risk Area	Risk Description
Legal & Compliance	Grants Management	Risk of noncompliance with federal and state grant requirements, including statutory, reporting, and financial obligations, which may result in questioned costs, repayment of funds, financial misstatements, loss of funding, or reputational harm.
Operational	Capital Asset Management	Risk that ineffective acquisition, tracking, maintenance, or disposal of capital assets may lead to financial inefficiencies, loss of resources, or inaccurate financial reporting.
Operational	Health & Safety	Risk that operational processes or workplace conditions may harm employees or the public, resulting in service disruptions, legal exposure, or reputational damage.
Operational	Information & Communication	Risk that ineffective communication, unclear procedures, or breakdowns in coordination may impair operational efficiency, decision-making, and service delivery.
Operational	Information Technology Controls	Risk of system failures, cybersecurity incidents, or inadequate protection of sensitive information that could disrupt operations or compromise data integrity.

Operational	Internal Controls	Risk that deficiencies in internal control systems may prevent timely detection or correction of errors, fraud, or noncompliance.
Regulatory	Regulatory Compliance	Risk of failure to comply with applicable regulations, which may result in sanctions, penalties, loss of authority, or reputational harm.
Strategic	Government Services	Risk that services may not align with statutory mandates or constituent needs, leading to inefficient resource allocation and reduced program effectiveness.
Strategic	Strategic Planning	Risk that unclear objectives or insufficient performance monitoring may hinder achievement of long-term goals.
Talent	Human Resource Management	Risk that ineffective workforce planning, recruitment, training, or retention may impair operational performance and long-term sustainability.

Statewide Risk Assessment Overview

The results of the 2025 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. 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. Overall, more than 80% of respondents indicated a high level of consensus and confidence in the existing controls and processes, as shown in Figure 2, which reports aggregate risk assessment results by category.

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



The management self-assessment indicates that Regulation is perceived as the area with the least amount of risk. This category shows that for 2025, agencies felt confident in their ability to actively monitor changes in regulations and assess their impact on existing policies and procedures. Additionally, agencies reported strong performance in ensuring changes are completed to existing policies to align with updated regulations, reviewed and then approved

by authorized personnel. 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 related to funding uncertainties, potential legislative changes that could impose new restrictions on agency functions, and the impact of demographic changes on service delivery and operational planning. Responses to these items suggest that agencies continue to view external fiscal, statutory and population-related dynamics considerations in their strategic and operational environments.

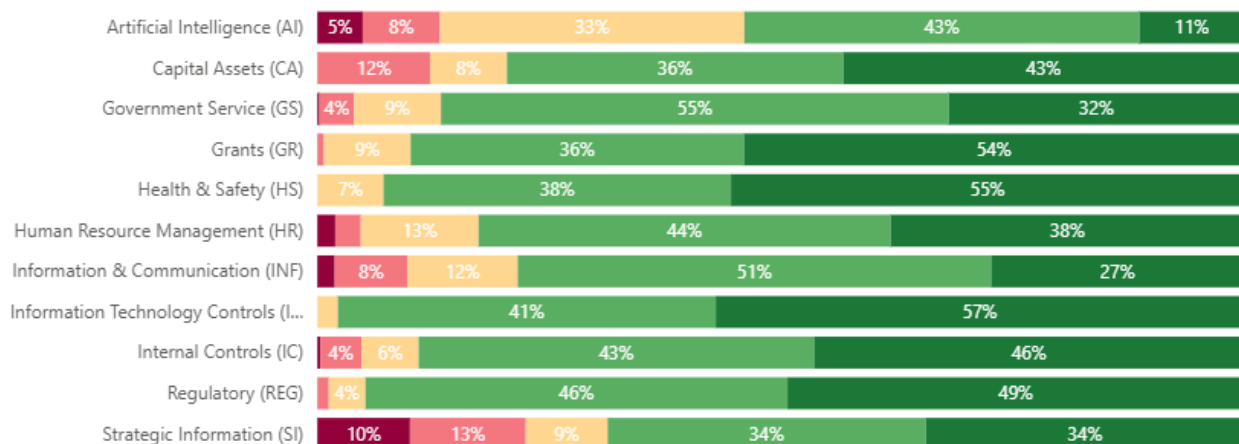
While the State's performance in Strategic Risk is relatively higher compared to other areas, the main concerns stem from external factors beyond the agencies' control. Budgetary uncertainty was most frequently provided in response as a potential threat to operational capacity. Agencies' responses indicate that stable and predictable funding remains central to maintaining service levels, staffing, and program continuity. Similarly, proposed legislative changes were also identified as an area of concern, reflecting the potential for shifts in statutory authority or regulatory requirements that could alter agency responsibilities, processes, or resource allocation. Lastly, agencies' feedback regarding demographic changes suggest awareness of evolving population trends, which could be geographic movement, age distribution, or service demand, that may require adjustments in planning, outreach, or program design to ensure continued effectiveness.

Though the State has demonstrated strengths in regulatory and legal areas, addressing the strategic risks identified could help improve the overall resilience and effectiveness of State and quasi-public 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

OIAPI took a closer look to identify any areas that may have scored higher in risk than others. To gain a more detailed understanding, OIAPI analyzed the risk scores by segment of the FIAA questionnaire, as shown in Figure 3 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 3: Statewide Risk Assessment – Full Survey Results by Segment



The Artificial Intelligence (AI) segment has risk score of 13%, which corresponds to the two red colors on the Likert scale. This score represents amongst the highest percentage of respondents who selected 'Strongly Disagree' and 'Disagree' indicating a higher perceived risk within this segment compared to the others. AI represents an emerging and rapidly evolving component that could affect agency operations, requiring thoughtful governance, clear oversight, and structured risk management to ensure responsible implementation. A high percentage in this segment could signify potential gaps in AI strategy, documentation, defined roles, risk evaluation, or compliance safeguards, which may increase exposure to data privacy concerns, bias, security risks, or inconsistent oversight as AI use expands.

OIAPI shared the list of surveyed agencies and their corresponding risk results with the following oversight entities:

- Enterprise Technology Strategy and Services (ETSS): Agencies that identified risks related to artificial intelligence or technology governance were referred to ETSS, which provides statewide IT leadership, oversight, and governance support.
- Division of Human Resources (HR): Agencies reporting risks related to human capital management were referred to HR, which oversees statewide personnel administration, workforce planning, and employee development.
- Division of Capital Asset Management and Maintenance (DCAMM): Agencies with identified risks related to capital assets or facilities management were referred to DCAMM, which manages and maintains the State's asset portfolio.

This approach ensures that when an agency identifies risk within a functional area governed by one of these oversight entities, the appropriate authority is informed and positioned to take proactive steps to address those concerns, even if the agency is not selected for inclusion in the upcoming audit plan.

Areas of Strength

Upon analyzing the FIAA survey results, certain risk areas were identified as strengths within the state agencies, with IT and Regulations standing out as areas of high performance. Though Regulatory compliance ranked as one of the lowest in risk, it is important to understand why this area was ultimately deemed a strength. State agencies demonstrated consistent processes for monitoring regulatory changes, assessing their impact, and updating internal policies and procedures accordingly. The presence of formal review and approval mechanisms, along with documentation practices, reflects a structured approach to maintaining compliance.

Agencies also indicated that they provide role-specific training and take steps to ensure policies are aligned with current regulatory requirements and implemented in a timely manner. This suggests not only awareness of compliance obligations, but also an operational commitment to embedding those requirements into daily practices. The combination of active monitoring, documented procedures, defined oversight and employee training contributed to the low-risk scores reported in this category and supports the conclusion that regulatory compliance is a relative area of strength.

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' 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 agencies 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. Additionally, ETSS recognizes the continued emergence of artificial intelligence technologies and is evaluating governance frameworks and internal controls to support responsible adoption and oversight across state agencies.

The State's approach to Health and Safety was another standout with a score of 93%. Agencies recognize the vital role of maintaining safe and secure environments for both employees and the public they serve. Responses indicate confidence in the effectiveness of emergency preparedness and response procedures as there are clear protocols and established communication channels during emergencies contribute to operational continuity and public trust.

The scores in Regulations, Information Technology and Health and Safety 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, OIAPI 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, rules, 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 controls.

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 23%, one percent lower than last year and ranking as the highest perceived risk category among the questionnaire segments. The questions posed to agencies ranged from strategic planning processes to Strengths, Weaknesses, Opportunities, Threats (SWOT) 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.

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.

Legislative changes can also have a considerable effect on strategic planning. Newly enacted legislation at both the federal and state level often lead to changes in mandates, regulations, 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 statutory and/or 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.

Lastly, artificial intelligence is an emerging area of consideration across certain agencies. As previously mentioned, survey results have been shared with ETSS leadership to support continued oversight, risk assessment, and responsible technology management as possible adoption evolves. The risks identified in both the operational and strategic segments provide insights that will help guide the structure of OIAPI's audit plan for FY 2027. By focusing on these areas in future audits, OIAPI can evaluate the root causes of these risks and provide recommendations to improve agencies' overall performance. The identified risk areas will guide the selection of agencies for inclusion in the upcoming audit plan, ensuring that OIAPI's efforts align with 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), OIAPI is required to conduct an audit of each quasi-public corporation at least once every five years.⁴ To comply with this mandate, OIAPI 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 the 2025 FIAA questionnaire as shown in Figure 4.

Figure 4: FY 2027 Required and Mandated Audits

Agency Name	Estimated Completion Date
Rhode Island Turnpike & Bridge Authority	Quarter 3
Rhode Island Convention Center	Quarter 3
Rhode Island Housing	Quarter 3
2026 FIAA Questionnaire	Quarter 4

OIAPI proposes including additional agencies in the FY 2027 audit plan. In addition to the FIAA results, OIAPI used other criteria to evaluate risk factors when selecting agencies to include in the FY 2027 audit plan, including:

- Increases and decreases in funding from the FY 2026 enacted budget and proposed FY 2027 budget;

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

- An evaluation of agency financial discipline through comparison of budgeted funds to actual expenditures;
- An evaluation of relative agency size through a comparison of budgeted funds; and
- Consideration is given to the length of time since the agency was last audited by OIAPI.

Based on the FIAA survey results, risk assessment, and feedback from the Internal Audit Advisory Group (IAAG), OIAPI plans to review the agencies identified in the FY 2027 proposed audit plan as shown in Figure 5.

Figure 5: OIAPI's FY 2027 Proposed Audit Plan

Agency Name
Department of Education
Department of Behavioral Healthcare, Developmental Disabilities and Hospitals
Department of Transportation
Rhode Island Emergency Management Agency
Department of Children, Youth, and Families
Department of Public Safety
Rhode Island College
Historical Preservation and Heritage Commission

It is important to note that this list remains a proposed audit plan and is subject for final approval by the IAAG. The proposed audit plan will be reviewed during the Q3 meeting and, upon approval, finalized for implementation in FY 2027.