

Board Packet List of Documents

Administrative & Audit Committee Meeting

Feb 18, 2025

- Meeting Agenda

- New Business
 - 1 2025 Board of Trustees Officers and Committee Assignments (Draft).
 - 2 Administrative & Audit Committee Charter
 - 2.1 Internal Audit Charter
 - 2.2 Ethics & Compliance Charter
 3. Internal Audit Update Report by KMH LLP
 - 4 Risk Assessment and Proposed Two-Year Internal Audit Plan Report by KMH LLP
 5. Compliance Support Staff Update Report

- APPROVAL OF MINUTES – October 23, 2024

Board Packet Documents are available for public for inspection on the Employees' Retirement System's Website: <https://ers.ehawaii.gov/board-and-committee-agendas-and-meeting-packets>; and in the Employees' Retirement System's Office, 201 Merchant Street, Suite 1400, Honolulu, HI 96813

NOTICE OF REGULAR MEETING

AGENCY: Administrative and Audit Committee of the
Board of Trustees of the Employees' Retirement System of the State of Hawaii

DATE: Tuesday, February 18, 2025; 2:00 p.m.

PLACE: City Financial Tower, 201 Merchant Street, Suite 1200, Honolulu, Hawaii 96813

The meeting will be conducted pursuant to HRS §92-3.7, under which Members of the Board of Trustees may participate via interactive conference technology; and members of the public may also participate via interactive conference technology or in person at the meeting place stated above.

Members of the public may also attend the meeting and provide testimony in person or by teleconference, either audio or video, at the following link or phone number:

https://teams.microsoft.com/l/meetup-join/19%3ameeting_YzRkMGQ1YjctOTZlZC00MTYyLTk2MDAtYmY1MTIwYzg0ZTkY%40thead.v2/0?context=%7b%22Tid%22%3a%223847dec6-63b2-43f9-a6d0-58a40aaa1a10%22%2c%22Oid%22%3a%228f795840-377f-479d-bb5d-6ec41c4a01bc%22%7d

Or join by entering meeting ID: 264 654 578 658

Passcode: 38wk2Mr6

Individuals testifying at the meeting are requested to limit their testimony to three (3) minutes or an amount of time otherwise designated by the Chairperson.

Or +1 808-829-4853 United States, Honolulu (Toll)
Conference ID: 226 373 864#

In the event audiovisual communication cannot be maintained with participating Trustees and quorum is lost, the meeting shall be automatically recessed for up to 30 minutes, during which time, an attempt to restore audiovisual communication will be made. If such attempt is unsuccessful, all Trustees, members of the public, staff and other interested individuals may continue to participate in the meeting via telephone using the above-listed telephone and conference ID numbers, whereby audio-only communication will be established for all participants and the meeting will continue. If reconvening the meeting is not possible because neither audiovisual nor audio-only communication can be re-established, the meeting will be terminated.

AGENDA

QUORUM/CALL TO ORDER

PUBLIC COMMENT

Members of the public may submit written testimony on these agenda items via e-mail or postal mail with receipt recommended by 4:30 p.m. on Monday, February 17, 2025, in order to ensure it is distributed in time for consideration. Please address written testimony if by e-mail to: dale.kanae@hawaii.gov or by postal mail to: Employees' Retirement System of the State of Hawaii, Board of Trustees, 201 Merchant Street, Suite 1400, Honolulu, HI 96813.

NEW BUSINESS

1. Discussion and Election of Chair and Vice Chair of the Administrative and Audit Committee.
2. Review and Discuss Revisions to the Administrative and Audit Committee, Internal Audit, and Ethics Compliance Charters to Include Administrative and Audit Committee Performance Assessment.

3. Internal Audit Update Report by KMH LLP on the Current Status of Activities Completed During Q4, 2024, and an Update on the Completion Status of Management Action Plans for Past Internal Audit Observations and Recommendations.
4. Risk Assessment Re-Evaluation and Proposed Two-Year Internal Audit Plan Report by KMH LLP. The Re-Evaluation and Plan Contain Proposed Assurance, Advisory, and Other Projects for 2025 and 2026.
5. Compliance Support Staff Quarterly Update Report on the Implementation of ERS' Compliance Program, Governance, Risk, and Compliance Platform, and Risk Strategy.
6. Update on Employer Reporting of Payroll Information Required by Act 87, SLH 2015.
7. Proposed Timetable Outlining the Process of the 2026 Trustee(s) Election for a General Employee and a Retirant.

Pursuant to HRS §92-5(a)(4), and (8), the Committee may enter into Executive Session to consider information that must be kept confidential pursuant to a state or federal law; and to consult with the Board's attorneys on questions and issues pertaining to the Board's powers, duties, privileges, immunities, and liabilities with respect to these matters.

APPROVAL OF MINUTES – October 23, 2024

EXECUTIVE SESSION

1. Executive Session, pursuant to HRS §92-5(a)(4) and (6), to consider and consult with the Board's attorneys on questions and issues pertaining to the Board's powers, duties, privileges, immunities, and liabilities, and to consider sensitive matters related to Cyber Security Updates.
2. Executive Session, pursuant to HRS §92-5(a)(8), to Review and Approve Executive Session Minutes of October 23, 2024.

ADJOURNMENT

If you require auxiliary aid/service or other accommodation due to a disability, please contact Dale Kehau Kanae at (808) 586-1706 or dale.kanae@hawaii.gov as soon as possible, preferably by Thursday, February 13, 2025, and the ERS will try to obtain the auxiliary aid/service or accommodation, but cannot guarantee that the request will be fulfilled.

Upon request, this notice can be made available in large print.

2025
BOARD OF TRUSTEES OF THE
EMPLOYEES' RETIREMENT SYSTEM
OF THE STATE OF HAWAII

OFFICERS & COMMITTEE ASSIGNMENTS

BOARD MEMBERS

Emmit Kane, Chair
Lance Mizumoto, Vice Chair
Vincent (Vince) Barfield
Catherine Chan
Genevieve (Genny) Gines Ley
David Louie
Luis Salaveria
Bennett Yap

ADMINISTRATIVE & AUDIT COMMITTEE (1/31/24)

Catherine Chan, Chair
Vincent (Vince) Barfield, Vice Chair
Genevieve (Genny) Gines Ley
Luis Salaveria

HUMAN RESOURCES COMMITTEE (2/12/24)

Vincent (Vince) Barfield, Chair
Genevieve (Genny) Gines Ley, Vice Chair
Catherine Chan
~~Luis Salaveria~~ David Louie

INVESTMENT COMMITTEE (2/20/24)

Lance Mizumoto, Chair
Bennett Yap, Vice Chair
Vincent (Vince) Barfield
Emmit Kane

LEGISLATIVE COMMITTEE (2/2/24)

Bennett Yap, Chair
Genevieve (Genny) Gines Ley, Vice Chair
Lance Mizumoto
~~Luis Salaveria~~ David Louie

GOVERNANCE POLICY COMMITTEE

Emmit Kane, Chair
(Board Chair)
Lance Mizumoto, Vice Chair
*(Board Vice Chair &
Investment Committee Chair)*
Vincent (Vince) Barfield
(Human Resources Committee Chair)
Catherine Chan
(Administrative & Audit Committee Chair)
Bennett Yap
(Legislative Committee Chair)

2024 Chair and Vice Chairs noted until selection for 2025.

Draft: Jan 13, 2025

Accepted:



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

I. PURPOSE

The Administrative & Audit Committee (“Committee”) of the Employees’ Retirement System (“ERS”) of the State of Hawaii is a committee of the Board of Trustees (“Board”). Its primary function is to assist the Board in fulfilling its oversight responsibilities relating to:

- A. The integrity of the ERS’s financial statements, accounting and financial reporting processes including internal and external audits;
- B. The ERS’s compliance with legal and regulatory requirements;
- C. The qualifications, independence and the performance of the ERS’s Internal and External Auditors;
- D. Monitoring the performance of the systems of internal controls established by Management and the Board;
- E. The business practices and ethical standards of the ERS;
- F. The review and monitoring of the administration of the ERS; and
- G. The review and monitoring of the Compliance Program.

The Committee provides an avenue of open and free communication between the Board, the Internal Auditors, the External Auditors, the Chief Compliance Officer, and Management of the ERS.

II. COMMITTEE MEMBERSHIP

- A. The membership of the Committee shall consist of at least three members of the Board.
- B. The Board members of the Committee shall be appointed annually by the Board Chair. Committee appointments can be changed at the discretion of the Board Chair at any time. In the event of a vacancy (due to member resignation, removal, or death), the Board Chair will appoint a replacement to serve the remainder of the term.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

- C. The members of the Committee shall be responsible for electing its Chair and Vice Chair.

III. MEETINGS

- A. The Committee must meet at least three (3) times per year or more frequently as circumstances require, with prior notice and publication of the agenda as provided by law.
- B. The Committee may ask members, ERS Management, advisors, and others to attend Committee meetings to provide pertinent information as necessary.

IV. AUTHORITY

The Committee shall have the power to conduct or authorize investigations into any matters within the Committee's scope of responsibilities. In the conduct of any investigation, the Committee shall have the authority to seek information it requires from ERS employees, Management, and external parties; and to engage advisors, or otherwise obtain independent legal, accounting, consulting, or other professional services it requires, at the expense of the ERS, with the approval of the Board.

V. RESPONSIBILITIES

The Committee provides oversight of various ERS functions: Administration, Risk Assessment, Internal Audits, External Audits, and Others. In fulfilling its oversight responsibilities, Committee members need to maintain an independent stance. Members of the Committee shall be considered independent if they have no relationship to the ERS that may interfere with the exercise of their fiduciary responsibilities.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

It is the duty of the Committee to report regularly to the Board with respect to any issues that arise concerning:

- A. The quality or integrity of the ERS's financial statements;
- B. The ERS's compliance with legal or regulatory requirements;
- C. The performance and independence of the ERS's External Auditors;
- D. The performance of the internal audit function;
- E. The allegations of serious suspected misconduct;
- F. Or any other matter within the scope of the Committee's function.

In carrying out its oversight responsibilities, the Committee's practices/procedures should remain flexible in order to best react to changing conditions and assure the Board that the risk assessment process, the accounting and financial reporting processes, internal controls, and internal and external auditing are in accordance with all related requirements and are of the highest quality.

Oversight Responsibilities Regarding Administration:

- A. Annually review the ERS strategic goals and objectives adopted by the Board and if appropriate, recommend any changes.
- B. Monitor Administration's implementation of these strategic goals and objectives.
- C. Provide direction to the Executive Director (ED) and Deputy Executive Director (DED) on priorities and actions to successfully execute the responsibilities of the Administrative Branch.
- D. Monitor compliance with administrative policies.
- E. Review and monitor the operating budget and provide recommendations to the full Board as necessary.

Oversight Responsibilities Regarding Risk Assessment:

- A. Inquire of Management, the Internal Auditors, and the External Auditors about significant risks or exposures.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

- B. Meet with the necessary parties to discuss the results of periodic risk assessments and obtain a clear understanding of the risk assessment process.
- C. Assess the steps Management has taken to minimize significant risks or exposures to the ERS.

Oversight Responsibilities Regarding Internal Audits:

- A. Where appropriate, oversee the procurement of internal auditing services and recommend to the Board:
 - 1. The Internal Auditor to be nominated;
 - 2. Approval of fees for the Internal Auditor; and
 - 3. The discharge of the Internal Auditor.
- B. Review the adequacy and effectiveness of the ERS's accounting and financial controls (including information technology and security controls) with:
 - 1. Personnel (from financial, accounting, and information systems);
 - 2. Internal and External Auditors; andelicit any recommendations to improve the system of internal controls or particular areas where new or more detailed controls or procedures are desirable.
- C. Obtain an understanding of any corrective actions to be taken with regard to controls and procedures.
- D. Recommend to the Board any co-sourcing or outsourcing internal audit services.
- E. Review the ERS Internal Audit Charter, including the independence and authority of the internal audit function, and its reporting obligations, qualifications, and staffing for the calendar year, and recommend its approval to the Board.
- F. Review the annual Internal Audit Plan (and all major changes to the plan) and recommend its approval to the Board.
- G. Review the reports and findings/recommendations of the Internal Auditors and the responses of the ERS Management, and monitors completion of Management's action plans.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

- H. Review a summary of major findings from completed internal audits and a progress report on the execution of the Internal Audit Plan and Management's implementation of action plans.
- I. Support the Chief Audit Executive through regular, direct communications.
- H. Meet separately with the Chief Audit Executive¹ and/or Management to discuss any matters that the Committee, or these parties, believe should be discussed privately.
- J. Review the effectiveness of the internal audit functions, including compliance alignment with the Institute of Internal Auditors' Global International Audit Standards for the Professional Practice of Internal Auditing.
- K. Report the results of the Internal Audit Plan to the Board. At the invitation of the Committee, the Internal Auditors will attend Board meetings to assist in reporting the results of the Internal Audit Plan and to answer questions.

Oversight Responsibilities Regarding External Audits:

- A. Obtain a basic understanding of government accounting, financial reporting, auditing processes, and critical policies, and ensure that the financial leadership team is qualified and competent.
- B. The State Office of the Auditor is responsible for the procurement of external auditing services and determines:
 - 1. The External Auditor to be nominated;
 - 2. Approval of the audit fees of the External Auditor; and
 - 3. The discharge of the External Auditor.
- C. Review prior year comments from the Government Finance Officers Association (GFOA) in its determination of the ERS's compliance with the requirements for the Certificate of Achievement in Financial Reporting, where applicable.
- D. Review with Management and the External Auditor the draft financial statements to be filed with the GFOA.

¹ The Chief Audit Executive may be an individual employee or a firm contracted to outsource or co-source the internal audit function.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

- E. Assess the integrity of the annual financial statements and related disclosures, including significant accounting judgements and estimates.
- F. Review and examine the independence (including any potential conflict of interest) of the External Auditor, including a review of Management consulting services and related fees provided by the External Auditor.
- G. Review with the External Auditor the coordination of audit effort to assure completeness of coverage, reduction of redundant efforts, and the effective use of audit resources.
- H. Review, at least annually, with Management and/or the External Auditor:
 - 1. Scope of the proposed audit for the current fiscal year and the procedures to be utilized.
 - 2. The ERS's annual financial statements and related footnotes.
 - 3. The External Auditor's audit of the financial statements and audit report thereon.
 - 4. The adequacy of the ERS's internal financial controls.
 - 5. Any significant changes required in the External Auditor's scope and audit plan.
 - 6. Other matters related to the conduct of the audit, which are to be communicated to the Committee under Generally Accepted Government Auditing Standards, including audit adjustments made and passed.
 - 7. Judgments about the quality, not just the acceptability of accounting principles and the clarity of the financial disclosures.
 - 8. Any difficulties encountered in the course of the external audits, including any disputes with Management, restrictions on the scope of their work or access to required information.
- I. Consider and review with Management any significant findings during the fiscal year and recommendations of the External Auditor's and Management's responses thereto.
- J. Meet separately with the External Auditor and/or Management to discuss any matters the Committee, or these parties, believe should be discussed privately with the Committee.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

- K. Report the results of the annual external audit to the Board. At the invitation of the Committee, the External Auditor will attend Board meetings to assist in reporting the results of the annual audit and to answer questions.

Oversight Responsibilities Regarding the Ethics and Compliance Program:

- A. Annually review the goals and objectives adopted by the Board and, if appropriate, recommend any changes.
- B. Periodically review the Ethics and Compliance Program Charter and make revisions, if necessary.
- C. Periodically evaluate the program and exercise reasonable oversight with respect to the implementation and effectiveness of the program.

Other Oversight Responsibilities:

- A. Report Committee actions, including any investigative actions, to the Board with such recommendations as the Committee may deem appropriate.
- B. Monitor the implementation of procedures for the receipt, retention and treatment of complaints regarding accounting, internal accounting controls, auditing or other matters, including mechanisms for anonymous submission of related concerns by ERS employees or the appropriate bodies.
- C. Consult with the Attorney General on legal matters regarding financial transactions, fraud, or any other issue that could have a significant impact on the annual reports.
- D. Obtain any information and training needed to enhance the Committee members' understanding of the role of Internal and External Auditors, the risk management process, internal controls and a certain level of familiarity in government financial reporting standards and processes.
- E. Obtain the Board's approval of this Charter and, on an annual basis, evaluate the adequacy of this Charter and recommend any proposed changes to the Board for approval.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ADMINISTRATIVE & AUDIT COMMITTEE CHARTER

- F. Confirm annually that the Committee has performed its responsibilities as outlined in this Charter.
- G. Coordinate with the Legislative Committee, Investment Committee, Governance Policy Committee, and Human Resources Committee, as deemed necessary.
- H. Perform such other functions as assigned by the Board.

VI. LIMITATIONS OF THE ADMINISTRATIVE AND AUDIT COMMITTEE'S ROLE

- A. It is not the duty of the Committee to plan or conduct audits or to determine that the ERS's financial statements are complete, accurate, and in accordance with Generally Accepted Accounting Principles. This is the responsibility of Management and the External Auditors.
- B. While the Committee is responsible for reviewing the ERS's policies and practices with respect to risk assessment and management, it is the responsibility of the Executive Director and Senior Management to determine the appropriate level of the ERS's exposure to risk.

Adopted and Approved by the Board of Trustees: June 12, 2012, August 10, 2020, April 11, 2022, March 13, 2023, March 11, 2024

Accepted by the Governance Policy Committee: March 28, 2022, March 7, 2023

Revised and Accepted by the Administrative & Audit Committee: July 21, 2020, February 9, 2022, February 22, 2023, January 31, 2024, February 18, 2025



Employees' Retirement System of the State of Hawaii BOARD OF TRUSTEES INTERNAL AUDIT CHARTER

I. INTRODUCTION

Internal auditing is an independent, risk-based, objective assurance and ~~consulting~~ advisory activity¹ designed to create, protect, and sustain add-value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The Internal audit function is most effective when:

- Internal auditing is performed by competent professionals in alignment with the Institute of Internal Auditor's Global Internal Audit Standards™, which are set in the public interest.
- The internal audit function is independently positioned with direct accountability to the Administrative & Audit Committee and Board of Trustees.
- Internal auditors are free from undue influence and committed to making objective assessments.

II. ROLE OF INTERNAL AUDIT

The Internal Audit function of the Employees' Retirement System ("ERS") is established by the ERS Board of Trustees ("Board") and its responsibilities are defined in this charter which is approved by the Board. The Chief Audit Executive ("CAE"), which may be an individual employee or a firm contracted to outsource or co-source

¹ As defined by the Institute of Internal Auditors, an *assurance* activity is an examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization, while ~~consulting-an advisory~~ activity refers to advisory-consulting and related client service activities intended to add value and improve an organization's processes.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
INTERNAL AUDIT CHARTER

the internal audit function, reports functionally to the ERS Administrative & Audit Committee (“Committee”) and administratively to the ERS Executive Director (“ED”) or designee. Approval from the Board is required for the hiring, compensation, removal, or replacement of the CAE.

The objectives of Internal Audit are to assist management and employees of the ERS in the effective discharge of their responsibilities by providing them with analyses, appraisals, recommendations, counsel, and information concerning the activities reviewed and to promote effective internal controls at a reasonable cost.

III. AUTHORITY

The CAE and the Internal Audit staff are authorized to:

- A. Review all areas of the ERS;
- B. Have full, free, and unrestricted access to all of the ERS’s activities, records, physical property, and personnel necessary to complete their work. Internal auditors are accountable for confidentiality and safeguarding records and information;
- C. Have full, free, and unrestricted access to the Board, Committee, ED, Deputy ED, Chief Investment Officer, Branch Chiefs, and all members of management;
- D. Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives; and
- E. Obtain the necessary assistance of personnel in units of the ERS where they perform audits, as well as other specialized services from within or outside the ERS.

The CAE and the Internal Audit staff are not authorized to:

- F. Perform any operational duties for the ERS;
- G. Initiate or approve accounting transactions external to the internal audit function; nor
- H. Direct the activities of any ERS employee not employed by the internal audit function, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
INTERNAL AUDIT CHARTER

IV. INDEPENDENCE & OBJECTIVITY

The CAE will ensure that the internal audit function remains free from all conditions that threaten the ability of internal auditors to carry out their responsibilities in an unbiased manner, including matters of engagement selection, scope, procedures, frequency, timing, and communication. If the CAE determines that objectivity may be impaired in fact or appearance, the details of the impairment will be disclosed to appropriate parties.

Internal auditors will maintain an unbiased mental attitude that allows them to perform engagements objectively such that they believe in their work product, do not compromise quality, and do not subordinate their judgment on audit matters to others, either in fact or appearance.

Internal auditors have no direct responsibility or any authority over any of the activities or operations that they review. They should not develop and install procedures, prepare records, or engage in activities that would normally be reviewed by internal auditors.

Internal Audit's objectivity is not adversely affected, however, by recommending standards of controls to be applied in developing systems and procedures, or by evaluating existing or planned financial and operating systems and related procedures, and making recommendations for modification and improvements thereto in order to improve controls and/or enhance operational effectiveness.

V. SCOPE OF WORK

The scope of ~~work of the Internal Audit function is to determine whether the ERS's network~~ internal audit activities encompasses, but is not limited to, objective examinations of evidence to provide independent assurance and advisory services to ERS and



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
INTERNAL AUDIT CHARTER

management on the adequacy and effectiveness of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Interaction with the various governance groups occurs as needed.
- Significant financial, managerial, and operating information is accurate, reliable, and timely.
- Employee actions are in compliance with policies, standards, procedures, and applicable laws and regulations.
- Operations are consistent with established goals and objectives.
- Operations are being carried out effectively, efficiently, ethically, and equitably.
- Resources are acquired economically, used efficiently, and adequately protected.
- Programs, plans, and objectives are achieved.
- Quality and continuous improvement are fostered in the ERS's control process.
- Significant legislative or regulatory issues impacting the ERS are recognized and addressed properly.

Opportunities for improving management control, process efficiency, and the ERS's image may be identified during audits. They will be communicated to the appropriate level of management.

VI. RESPONSIBILITIES

Internal Audit is responsible for the following activities:



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
INTERNAL AUDIT CHARTER

Standards

- A. ~~The CAE is responsible for ensuring that all activities of the internal audit function are carried out in compliance with the Institute of Internal Auditors' ("IIA") mandatory guidance including the "Definition of Internal Auditing," the "Code of Ethics," and applicable standards found in the "International Standards for the Professional Practice of Internal Auditing."~~ Ensure internal audit engagements are performed, documented, and communicated in alignment with the Global Internal Audit Standards and laws and/or regulations.
- B. Conduct a periodic risk assessment for the ERS and present the results to the Committee.
- C. ~~Develop a flexible annual Internal Audit Plan using an appropriate risk-based methodology~~ Biennially develop a two-year risk-based internal audit plan, which considers risks or control concerns identified by management, and submit the plan to the Committee and the Board for review and approval. Review and adjust the internal audit plan with appropriate approval by the Committee, as necessary.
- D. Implement the annual Internal Audit Plan, as approved, including, and as appropriate, any special tasks or projects requested by management, the Committee, and the Board.

Ethics

- E. Review the adequacy of the ERS's adopted code of conduct activities, including the process to receive, retain, and treat complaints received on accounting and auditing matters.
- F. Monitor management's process for ensuring compliance with Hawaii Revised Statutes – Chapter 84, Standards of Conduct ("State Ethics Code").



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
INTERNAL AUDIT CHARTER

Monitoring & Follow-Up

- G. Evaluate any plans to correct reported conditions for satisfactory improvement of the business process.
- H. Provide adequate follow-up to ensure corrective action is taken and evaluate its effectiveness before recommending closure of an issue.
- I. Monitor and evaluate the effectiveness of the organization's risk management processes.

Reporting

- J. Prepare and issue a written report following the conclusion of each audit and follow-up audit. This report shall include significant findings, recommendations to management, and management's action plan. A copy of the report will be forwarded to the Committee, ED, Deputy ED, Chief Compliance Officer, and appropriate members of management.
- K. Inform and advise management and the Committee as to significant deficiencies or other substantive issues noted in the course of its activities.
- L. Provide periodic reports on Internal Audit's progress on implementing the annual Internal Audit Plan, including management's progress on addressing previously reported matters, the impact of resource limitations, and significant interim changes.
- M. On a regular basis, the CAE will meet separately with the Committee to discuss any matters that is deemed necessary by the Committee or Internal Audit.

Other

- N. Conduct special examinations at the request of management or the Committee.
- O. Perform consulting services, beyond internal auditing assurance services, to assist management in meeting its objectives. Examples may include facilitation, consultation on internal control improvement initiatives, training, and advisory services.



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
INTERNAL AUDIT CHARTER

- P. Assist in the investigation of significant suspected fraudulent activities within the organization and notify management and the Committee of the results.
- Q. Evaluate and assess significant merging/consolidating functions and new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion.
- R. Keep the Committee informed of emerging trends and successful practices in internal auditing.
- S. Review this Internal Audit Charter on an annual basis to ensure the purpose, authority, and responsibilities of Internal Audit continue to be adequate in accomplishing its objectives. Modify as appropriate and submit to the Committee and ED for review and approval.

Adopted and Approved by the Board of Trustees: June 12, 2012, April 11, 2022, March 13, 2023, March 11, 2024

Accepted by the Governance Policy Committee: March 28, 2022, March 7, 2023

Revised and Accepted by the Administrative & Audit Committee: June 9, 2020, February 22, 2023, January 31, 2024, February 18, 2025



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ETHICS & COMPLIANCE CHARTER

I. INTRODUCTION

The Employees' Retirement System ("ERS") Ethics and Compliance function is an independent monitoring, advisory, review, and reporting activity established within ERS to assist the organization in fulfilling its mission, vision, and fiduciary responsibilities by complying with laws, regulations, and ERS policies, for which oversight has been assigned. The function strives to ensure, promote and support an organizational culture that builds ethics and compliance awareness into the daily business processes for ERS. ERS's Compliance Program will accomplish this mission by monitoring business activities, policies and procedures, and by establishing an infrastructure that provides additional assurance to management that program areas are in compliance.

The Chief Compliance Officer ("CCO") is authorized to engage in independent reviews and activities for the development and implementation of a comprehensive system of operational controls to prevent illegal, unethical, or improper conduct and to implement compliance policies and procedures relating to standards of ethics and conduct for ERS' Board, employees, and vendors.

II. ROLES & RESPONSIBILITIES

Under the direction of the Executive Director ("ED") and oversight of the Board, the CCO:

- A. Pursuant to the Ethics and Compliance Program Charter, manages day-to-day operation of the compliance program;
- B. Monitor and assess the Policy Management Framework and oversee the completion of the Policy Lifecycle;
- C. Assesses and audits ERS' controls and compliance with all applicable laws, statutes, administrative rules, regulations and best practices outlined in policies;



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ETHICS & COMPLIANCE CHARTER

- D. Collaborates with other divisions to implement compliance policies and procedures and to direct compliance issues to appropriate channels for investigation and resolution;
- E. Collaborates with the Information Technology Branch Chief to build a strategic security program and coordinates all phases of security projects from requirement definition to design, architecture, implementation, testing, support, and maintenance;
- F. Develops and periodically reviews and updates standards of ethics and conduct to ensure that continuing effective guidance is provided to the Board, management, and employees;
- G. Coordinates with the Department of the Attorney General on legal matters so that ERS may faithfully execute its duties and responsibilities;
- H. Coordinate with the Internal Auditor to monitor and provide independent oversight over the implementation of the approved annual Internal Audit Plan;
- I. Coordinates with management, the Committee, and the Board on any special tasks or projects aligned with the long-term interests of ERS;
- J. Ensures that compliance issues and concerns within the organization are being appropriately evaluated, investigated, and resolved;
- K. Coordinate audit efforts with those of the ERS's external auditors and other regulatory agencies;
- L. Responds to alleged violations of rules, regulations, policies, procedures, and standards of ethics and conduct by evaluating and, if necessary, recommending the initiation of investigative procedures;
- M. Develops and oversees a system for uniform handling of such violations;
- N. Identifies potential areas of compliance vulnerability and risk;
- O. Develops/implements corrective action plans for resolution of problematic issues and provides general guidance on how to avoid or deal with similar situations in the future;



Employees' Retirement System of the State of Hawaii
BOARD OF TRUSTEES
ETHICS & COMPLIANCE CHARTER

- P. Works in coordination with management and the Branch Chiefs to develop, maintain, and test the disaster recovery, business continuity, risk management and access control needs of the organization;
- Q. Provides reports as directed or requested to keep the Board, Administrative & Audit Committee, and management informed of the operation and progress of compliance efforts;
- R. Ensures proper reporting of violations or potential violations to duly authorized enforcement agencies as appropriate and/or required; and
- S. Works with the Board, Administrative & Audit Committee, Internal Auditor, Department of the Attorney General, and management to develop an effective compliance training program for Board Members, managers, and employees, including appropriate introductory training for new employees.

In carrying out these responsibilities, the CCO shall:

- A. Ensure objectivity and independence;
- B. Remain free of actual or perceived conflicts of interest;
- C. Discharge professional responsibilities with due care, competence, and diligence;.
- D. Have access to all functions, records, property, and personnel necessary to complete responsibilities; and
- E. Have full and free access to the Board and the Administrative & Audit Committee.

III. CHARTER REVIEW & HISTORY

The Administrative & Audit Committee shall, on behalf of the Board, review this Charter at least annually to ensure it remains relevant and appropriate.

Adopted and Approved by the Board of Trustees: March 13, 2023, March 11, 2024

Accepted by the Governance Policy Committee: March 7, 2023

Introduced and Accepted by the Administrative & Audit Committee: February 22, 2023, January 31, 2024, February 18, 2025

Employees' Retirement System INTERNAL AUDIT



Employees' Retirement System
of the State of Hawaii

ADMINISTRATIVE & AUDIT COMMITTEE UPDATE REPORT

February 18, 2025

CONFIDENTIAL

This report is prepared solely for the internal use of the Employees' Retirement System management, the Administrative & Audit Committee, and the Board of Trustees. Distribution requires prior approval from the Administrative & Audit Committee or management.



TABLE OF CONTENTS

SECTION	PAGE
Executive Summary	1
Global Internal Audit Standards Summary	4
2024 Internal Audit Plan Results Summary	6
Management Action Dashboard	7
Management Action Plans – Completion Status	9
Cumulative Observation Analysis	10
Issued Reports Finding Status	11
Appendix A: Virtual Chief Information Security Officer (vCISO) Bio	44



Executive Summary

Administrative and Other Matters

- Internal Audit (“IA”) continues to regularly meet with Executive Management to keep them apprised of current and upcoming IA projects and discuss new or updated needs of the organization.
 - Met with Executive Management in January 2025 to introduce ourselves to the new Deputy Executive Director and provide an introduction, history and background of the IA function.
- Continue to meet with the Chief Compliance Officer (“CCO”) on a weekly basis to stay apprised on current ERS and CCO initiatives, emerging risk areas, challenges and issues, and upcoming events and other matters.
- IA has suggested revisions to the ERS’ Internal Audit and Administrative & Audit Committee Charters to align with the new Global Internal Audit Standards, effective January 9, 2025. IA’s methodology has been updated using the new Standards, specifically revising references/mapping from the prior standards and updating for new terminology/definitions.
 - **Action: Seeking approval from Administrative & Audit Committee of revised Internal Audit Charter and Administrative & Audit Committee Charter**

Status on Current Projects:

Virtual Chief Information Security Officer (vCISO)

- Ty Smith, RSM Director, replaced Dave Collins in February 2025 as ERS’ vCISO.
- He has met with the Executive Director and Deputy Executive Director and in the process of meeting with ERS staff. He has been working with the RSM team (including Dave) on transition and has been able to “hit the ground running”.
- The “vCISO Initiative – Roadmap Implementation” project will be led by Ty.
- See detailed resume in *Appendix A*.



Status on Current Projects (cont'd):

Investment Manager Selection and Evaluation Review

- Currently in post-fieldwork internal review and reporting.
- The review objectives are to:
 - Evaluate the Investment Office's compliance with the requirements and internal controls set forth in the ERS' Investment Manager Selection Process Framework; which is comprised of stages to identify, evaluate, recommend, and approve prospective investment managers.
 - Assess whether the ERS' Investment Manager Selection Process Framework aligns with leading practices recommended by professional investment organizations and/or performed by peer pension systems in order to identify opportunities to enhance the current framework.
 - Provide recommendations and leading practices for improvements to enhance effectiveness and efficiency, where applicable.
- As part of this review, IA met with two of ERS' Investment Consultants to obtain feedback on the current selection framework and used the Institutional Limited Partners Association (ILPA) and the CFA Institute as leading professional investment organizations for comparison.
- Estimated final report issuance and review completion is March 2025.

Contracting & Procurement Review

- Currently in the internal planning and project-level risk assessment phase.
- Walkthrough meetings with those involved in contracting and procurement will begin in March 2025.
- Scope will include assessing ERS' procurement lifecycle and structure as well as compliance with applicable statutes including Hawaii Revised Statutes Chapter 103D, referred to as the State's Public Procurement Code.



Status on Current Projects (cont'd):

Risk Assessment Re-Evaluation & Two-Year Internal Audit Plan

- The Risk Assessment Re-Evaluation & Two-Year Internal Audit Plan process was completed in January 2025 and includes the proposed 2025-2026 Internal Audit Plan.
- Held individual meetings with the Executive Team, Branch Chiefs, Board of Trustees, and External Auditor to discuss changes within their respective areas of responsibility and identify new and emerging risks.
- Risk Assessment Re-Evaluation and Proposed Two Year Internal Audit Plan Report is included herein with current Administrative & Audit Committee materials.

Action: Seeking approval from Administrative & Audit Committee of proposed 2025-2026 Internal Audit Plan



Global Internal Audit Standards Summary

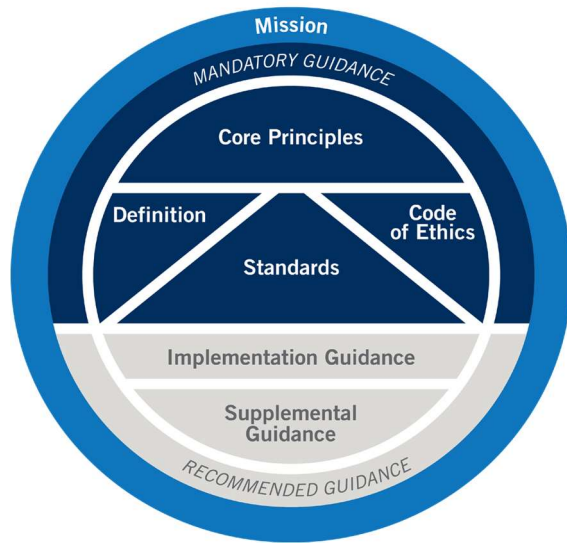
The Global Internal Audit Standards (“Standards”), effective January 2025, guide the worldwide professional practice of internal auditing and serve as a basis for evaluating and elevating the quality of the internal audit function.

Prior to the Standards, the professional practice of internal auditing was guided by the 2017 International Standards for Professional Practice of Internal Auditing and the mandatory guidance of the International Professional Practices Framework (IPPF), which included the Code of Ethics, Core Principles for the Professional Practice of Internal Auditing, Definition of Internal Auditing, and Mission of Internal Audit. The Standards incorporated the content from the standards and guidance into one resource.

2017



International Professional
Practices Framework



2024



International
Professional Practices
Framework®
(IPPF)



Global Internal Audit Standards Summary (continued)

The Standards include 5 Domains, 15 Principles, and 52 Standards that define each domain. Internal auditors are required to conform with the Principles and supporting Standards covered in each domain.

5 Domains, 15 Principles

Domain I: Purpose of Internal Auditing

II. Ethics and Professionalism

1. Demonstrate Integrity
2. Maintain Objectivity
3. Demonstrate Competency
4. Exercise Due Professional Care
5. Maintain Confidentiality

III. Governing the Internal Audit Function

6. Authorized by the Board
7. Positioned Independently
8. Overseen by the Board

IV. Managing the Internal Audit Function

9. Plan Strategically
10. Manage Resources
11. Communicate Effectively
12. Enhance Quality

V. Performing Internal Audit Services

13. Plan Engagements Effectively
14. Conduct Engagement Work
15. Communicate Engagement Conclusions and Monitor Action Plans



2024 Internal Audit Plan Results Summary

Internal Audit Plan Period: January 1, 2024 through December 31, 2024																
PROJECT	Q1 2024			Q2 2024			Q3 2024			Q4 2024			Hours			
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Budget*	Actual*	ETC*	Variance*
IA 2023 Carryover Projects																
Member Enrollment & Re-Enrollment Review													100	118	-	18
Continuous Monitoring Tool Development - Part 1													85	93	-	8
Business Continuity Plan – Crisis Communication Plan Development													100	91	-	(9)
IA Assurance																
Follow-Up Review													300	303	-	3
Investment Manager Selection & Evaluation Review													400	280	150	30
Contracting & Procurement Review													400	32	375	7
IA Advisory & Other																
Virtual Chief Information Security Officer (vCISO)													300	318	-	18
Implementation of Cybersecurity Strategy and Roadmap (moved to 2025)													350	3	-	(347)
Continuous Monitoring Tool Development - Part 2 (moved to 2025)													250	29	-	(221)
Compliance Office Collaboration and Assistance	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	150	224	-	74
IA Recommendation & Implementation Assistance	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	100	-	-	(100)
Risk Assessment Re-Evaluation & Audit Plan for Year 3 & Year 4										◆	◆	◆	250	117	135	2
Reporting, Communication and Other Administration	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	250	328	-	78
Total Hours													3,035	1,936	660	(439)

◆ Project Start Date
 In Process
 Draft Report Issued - Pending Mgmt Responses and/or A&AC Approval
 Completed - Final Report or Deliverable Issued
 ◆ ◆ Consulting & Other Projects
 ◆ - ◆ Meetings, Board Support, Other

Key: Budget: Original Approved Budget and Budget Changes Approved by the Administrative & Audit Committee
 Actual: Actual Hours Incurred Through December 31, 2024
 ETC: Estimated Time to Complete
 Variance: [(Actual + ETC) - Budget] = over / (under) budget



Management Action Dashboard

The following represents the status of IA reports with open findings and recommendations.

Name of Review	Contact	Overall Rating ¹	Total Number of Findings	Number of Findings Ranked			Completion Status (Only "High" and "Moderate" / "Medium" findings were tracked for the first four projects listed below)					
				"High"	"Moderate" or "Medium"	"Low"	Cleared	Outstanding - Not Overdue	Outstanding - Extended Original Target Date	Outstanding - Funding Shortfall	Overdue	Mgmt Chose Not to Implement
IT Security Rapid Assessment & Internal Network Security Review ("INSR")	IT Manager	Unacceptable	12	6	6	0	9	0	0	0	3	0
Cash & Liquidity Management Review	Accounting Manager	Marginal	4	0	3	1	0	0	0	0	3	0
Financial Reporting Process Review	Accounting Manager	Marginal	5	1	4	0	2	0	0	0	3	0
Human Resources - Personnel Development & Retention Review	Deputy Executive Director	Generally Satisfactory	2	0	2	0	1	0	0	0	1	0
Cloud Risk and Security Assessment - Phase 1	IT Manager	Marginal	5	0	4	1	0	0	5	0	0	0
Employer Communication & Reporting Review	Retirement Benefits Manager, Accounting Manager, Program Specialist	Marginal	3	0	2	1	2	0	1	0	0	0
Cloud Risk and Security Assessment - Phase 2	IT Manager	Unacceptable	5	4	1	0	0	0	4	0	1	0
Member Enrollment & Re-Enrollment Review	Retirement Benefits Manager, SSS Supervisor, IT Manager	Unacceptable	5	2	3	0	1	1	3	0	0	0
TOTAL			41	13	25	3	15	1	13	0	11	0



Management Action Dashboard (continued)

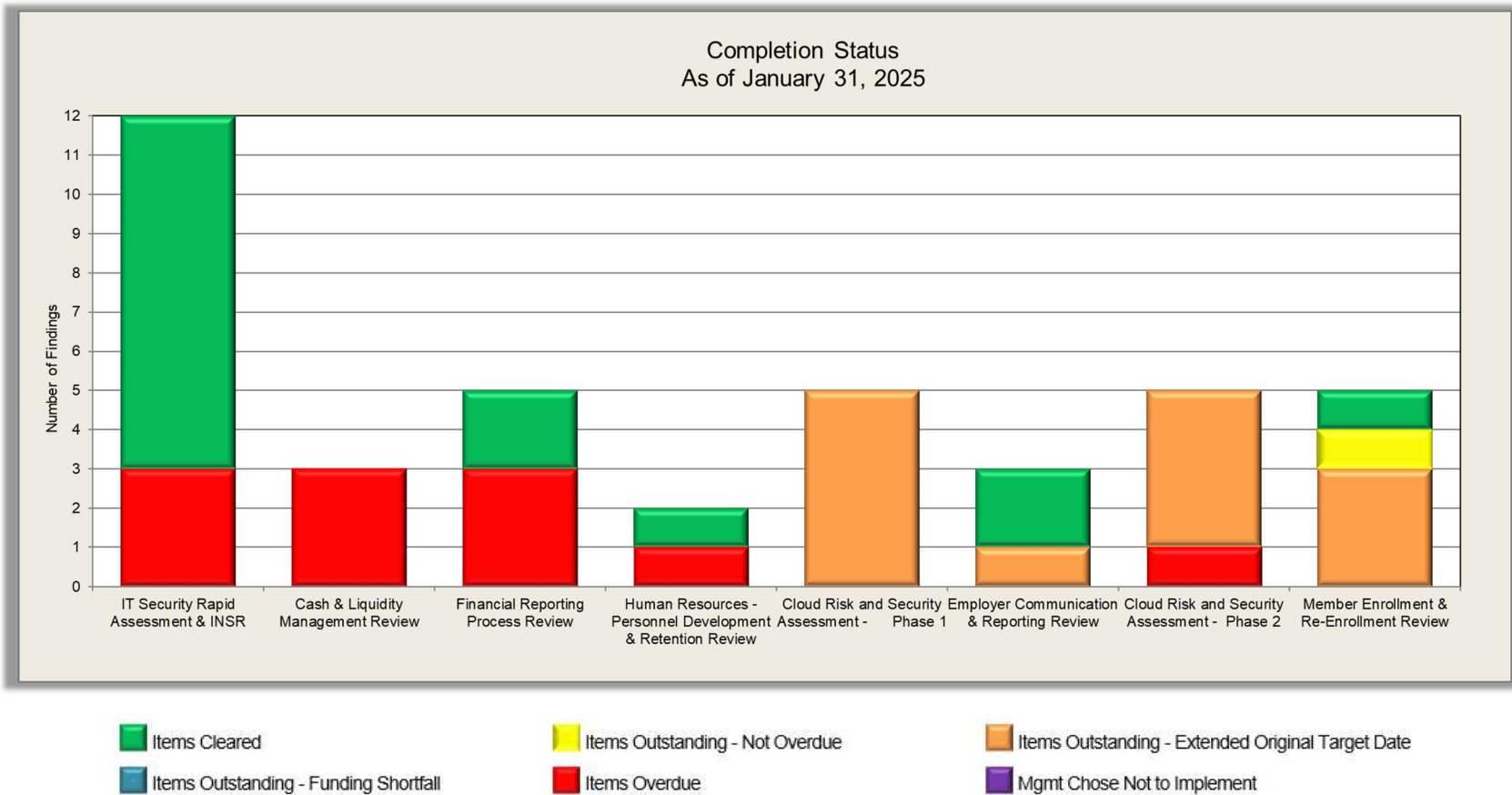
¹ Overall Rating Definitions:

- **Strong** – The area reviewed has effectively assessed and managed its risks, implemented control processes, and complied with applicable policies, procedures, and appropriate laws and regulations. Internal control systems are sufficiently comprehensive and appropriate to the size and complexity of the organization. Monetary risk associated with control failures, if any, is not material. A few inconsistencies may have been noted, but compensating controls exist that sufficiently minimize the risk of loss (e.g., financial, reputational).
- **Generally Satisfactory** – The area reviewed has adequately assessed and managed its risks, and has implemented generally effective control processes. Some weaknesses in controls may have been noted, but they are not such that the area is significantly exposed to risk of loss. Weaknesses or deficiencies identified are correctable in the normal course of business. Such areas are in general compliance with applicable policies, procedures, and appropriate laws and regulations.
- **Marginal** – The area reviewed has control, policy, procedural, compliance and/or repeat findings that are sufficiently important to warrant the attention of more senior levels of management. Any deterioration in the current operating routine could lead to serious exposures and stakeholder criticisms. Should weaknesses continue without attention, they could lead to further deterioration of the rating to an *unacceptable* status.
- **Unacceptable** – The area reviewed has serious control, policy, procedural, compliance and/or repeat findings. Exposure to potentially serious risk of loss exists. Exposure may also exist to potentially serious criticism by stakeholders. Such situations require urgent senior management involvement in implementing corrective action. Corrective action should be initiated immediately and may require significant amounts of time and resources to implement.



Management Action Plans – Completion Status

The following represents the number of findings that are cleared; outstanding – not overdue; outstanding – funding shortfall; findings for which there have been extensions granted; findings for which management chose not to implement; and overdue for each review. After the granting of two extensions, if the finding is not cleared, it will be shown as overdue.





Cumulative Observation Analysis

Based on the 23 reviews completed over the last few years, we compiled a listing of common observations across the reviews. Management is currently in the process of addressing these organization-wide improvement opportunities.

Common Observations					
	Areas for Improvement				
	Oversight & Monitoring	Policies and/or Procedures	Obtaining Appropriate Resources	Developing Efficient Processes	
Reports Issued	Member Enrollment & Re-Enrollment Process Review	X	X	X	X
	Records Management & Retention Review	X	X		X
	Investment Manager Selection & Evaluation Review		X	X	X
	Access Controls Review	X	X	X	
	Data Collection & Maintenance Review	X	X		X
	Member Retirement Application & Eligibility Review	X	X		X
	Unclaimed Member Benefits & Accounts Review	X	X		X
	Benefit Disbursement Review	X	X		X
	Governance & Ethics Review	X	X	X	
	IT Security Rapid Assessment & INSR	X	X	X	
	Cash & Liquidity Management Review	X	X	X	
	Disability Hearings and Contested Cases Review	X	X	X	
	Investment and Risk Monitoring and Reporting Review	X	X		X
	Financial Reporting Process Review	X	X	X	X
	Investment Consultant Selection and Evaluation	X			X
	Communications and Community Relations Review		X	X	X
	Human Resources - Personnel Development & Retention Review		X	X	
	Cloud Risk and Security Assessment - Phase 1	X	X	X	
	Benefit Estimates & Final Benefit Calculation Processing Review			X	
	Employer Communication & Reporting Review	X	X		X
	Cloud Risk and Security Assessment - Phase 2	X	X	X	X
	Member Enrollment & Re-Enrollment Review	X	X	X	X

*No observations were noted in the Investment Governance Structure & Oversight Review.



Issued Reports Finding Status

The following represents a summary of the recommendations from the respective issued and final reports, with targeted implementation dates and a brief status **provided by management**. For all reports issued in 2019 (starting with the Financial Reporting Process Review) and on a go-forward basis, IA will track recommendations for all findings (“High”, “Medium”, and “Low”). Once recommendations are considered “cleared”, they will be removed from this status tracking.

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
IT Security Rapid Assessment & Internal Network Security Review				
Note: The progress and status of Finding 2 of this review is tracked through the Cloud Risk and Security Assessment Phase 1 - Finding 3 due to overlapping recommendations. The clearing of the recommendations in Finding 3 will also clear Finding 2 .				
<p>Finding 6 – A number of instances were identified where a Man-in-the-Middle (“MitM”) attack is possible, allowing an intruder to secretly relay and possibly alter the communications between two parties, as well as to gain potentially elevated access in an unauthorized manner.</p>	<p>Management should evaluate the benefits of adding a Security Information and Event Management (“SIEM”) system or similar form of network monitoring system to detect network sniffing and Server Message Block (“SMB”) relay attacks. Using NTLM v2 hashing can lower the risk of these types of attacks against the network, but does not prevent sniffing.</p>	High	<p>June 2017 (Revised #1 Target Date: December 2017) (Revised #2 Target Date: December 2020) (Revised #3 Target Date: December 2021) (Revised #4 Target Date: December 2022) (Revised #5 Target Dates: September 2023, TBD) (Revised #6 Target Date: June 2024) Revised #7 Target Date: TBD)</p>	<p>Outstanding – Overdue – ERS is working with a Virtual Chief Information Security Officer (vCISO). Due to the significant number of vacancies in the I/S branch, Target Date is TBD for implementation of SIEM / Managed Detection and Response (MDR) solution and evaluation of the Server Message Block (SMB).</p> <p>The status update below applies to all outstanding IT-related findings</p> <p>Over the last 5 months not much has changed staffing wise. We conducted numerous interviews and have been unable to fill key</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
				<p>vacancies. In fact, the systems & applications sections each lost one staff member causing the vacancy rate to increase to over 50%.</p> <p>To help ensure progress is being made in a strategic way, there are plans to develop a Security Steering Committee that will help prioritize the many outstanding security items and will also take into consideration current Operations projects such as the Pension Administration System migration, compliance software implementation, etc. The committee can also assist with obtaining needed resources whether it be hiring, procuring services or outsourcing. The committee can also assist with holding people more accountable, especially as it relates to procurement.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
				<p>Note: We were advised that the vCISO that we were working with has left the organization and that we will be assigned a new one. This will cause a delay to our plans.</p>
<p>Finding 8 – There is no formal Software Development Lifecycle (“SDLC”) or Change Management policy in place to govern changes in the production environment and related security impacts.</p>	<p>The ERS should create a risk framework that rates each development/engineering project as well as system change. The risk framework should factor in regulatory and customer commitments and requirements as they relate to IT security. The assigned risk rating to each project or change would then dictate the level of security considerations to be incorporated.</p> <p>Formalized change policies and procedures should be established as well to address segregation of duties risks.</p>	<p>Moderate</p>	<p>June 2017 (Revised #1 Target Date: December 2021) (Revised #2 Target Date: September 2022) (Revised #3 Target Date: June 2024) (Revised #4 Target Date: TBD)</p>	<p>Outstanding – Overdue – Due to the significant number of vacancies in the I/S branch, Target Date is TBD for ERS administrative governing policies and a schedule for the finalization of I/S policies will follow.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
Cash & Liquidity Management Review				
<p>Finding 1 – There is no formal cash management framework. While there are some elements of a cash management framework in place, based on industry standard resources reviewed, key features of cash management are missing.</p>	<p>Management should develop a formal cash management framework including the following elements:</p> <ol style="list-style-type: none"> 1) An organization-wide cash management policy, 2) Implementation of software to assist in preparing formal cash forecasts, 3) Definition of key components of cash forecasting, and 4) Establish reporting protocols. 	<p>Moderate</p>	<p>September 2017 (Revised #1 Target Date: June 2020) (Revised #2 Target Date: December 2021) (Revised #3 Target Date: December 2024) (Revised #4 Target Date: December 2025)</p>	<p>Outstanding – Overdue – Funding request was not submitted for FY2026 due to other ERS priorities.</p> <p>ERS Investments has implemented Cash Overlay Program with ERS investment consultants and custodial bank to monitor ERS cash requirements.</p> <p>ERS Accounting and Investments will review cash management framework during the next six months to determine future reporting requirements.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
<p>Finding 2 – There is no formal process or methodology in place to determine the optimal monthly cash reserve that meet immediate cash obligations and also maximize higher earning investments.</p>	<p>Accounting should establish specific guidelines for evaluating the cash reserve, such as:</p> <ol style="list-style-type: none"> 1) Frequency of evaluation, 2) Line items to be reviewed for adjustment, 3) Threshold amounts, 4) Triggering events that could result in immediate change, and 5) Investing temporary surpluses productively. 	<p>Moderate</p>	<p>September 2017 (Revised #1 Target Date: June 2020) (Revised #2 Target Date: December 2021) (Revised #3 Target Date: December 2024) (Revised #4 Target Date: December 2025)</p>	<p>Outstanding – Overdue – Refer to status comment for Finding 1 above.</p>
<p>Finding 3 – There is no comprehensive cash forecasting process. In addition, variance analyses and updates to line items are not made throughout the year.</p>	<p>ERS should:</p> <ol style="list-style-type: none"> 1) Reevaluate current cash forecasting processes, 2) Establish a collaborative formal cash flow forecasting process, led by an individual with treasury experience, 3) Provide cash projections to all involved departments, and 4) Set tolerance levels of variance between actual and projected forecasts. 	<p>Moderate</p>	<p>September 2017 (Revised #1 Target Date: June 2020) (Revised #2 Target Date: December 2021) (Revised #3 Target Date: December 2024) (Revised #4 Target Date: December 2025)</p>	<p>Outstanding – Overdue – Refer to status comment for Finding 1 above.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
Financial Reporting Process Review				
<p>Finding 3 – Financial reporting policies and procedures have not been reviewed or updated since the 1990s.</p>	<p>The Accounting Branch should draft a set of updated policies and procedures for the financial reporting process areas. Policies and procedures should be established for the following:</p> <ul style="list-style-type: none"> ▪ Annual financial audit and CAFR preparation ▪ Monthly financial statement activities ▪ Financial statement preparation and distribution ▪ Management reports (internal) 	Moderate	<p>June 2020 (Revised #1 Target Date: December 2021) (Revised #2 Target Date: December 2024) (Revised #3 Target Date: December 2025)</p>	<p>Outstanding – Overdue – ERS will seek the necessary resources to assist in the development of policies, procedures, and related training.</p> <p>Refer to statuses provided for the Cash & Liquidity Management Review related to the timing of obtaining a third-party consultant.</p>
<p>Finding 4 – Accounting policies and procedures have not been adjusted to maintain alignment with the changing Investment Policy and shifts in the investment portfolio.</p>	<p>The Investment Office should actively involve and discuss potential investments with the Accounting Branch.</p> <p>The Accounting Branch should develop the appropriate policies, procedures and controls to align with any shifts in the investment portfolio.</p> <p>Management should also consider sending both Investment Office and qualified</p>	Moderate	<p>June 2020 (Revised #1 Target Date: December 2021) (Revised #2 Target Date: December 2024) (Revised #3 Target Date: December 2025)</p>	<p>Outstanding – Overdue – Draft policy template received from KMH.</p> <p>Detailed policies and procedures may require funding for necessary resources to assist in the development of policies, procedures, and related training as part of 2024 Legislative Session.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	Accounting Branch personnel to on-site due diligence visits for select high valuation risk investments.			Refer to statuses provided for the Cash & Liquidity Management Review related to the timing of obtaining a third-party consultant.
<p>Finding 5 – Work report data files are consistently submitted by the employer groups with errors and in improper formatting. ERS resources, particularly the Accounting Branch and EC&B, are spending a significant amount of time correcting these errors which leads to delays in financial reporting.</p>	<p>ERS is meeting with representatives of employer groups to discuss improving reporting. In addition to this effort, ERS should complete the following:</p> <ul style="list-style-type: none"> ▪ Developing IT scripts specific to individual employer submissions that may be able to identify common errors. ▪ Establishing an ERS help-line to coordinate training and support for different employer groups. Also, ERS can go to the individual employer work locations to conduct training on work report data files. 	Moderate	<p>December 2020 (Revised #1 Target Date: December 2022) (Revised #2 Target Date: December 2024) (Revised #3 Target Date: TBD)</p> <p>**Progress is evaluated on an on-going basis and it is unrealistic to determine a due date. See status comments.</p>	<p>Outstanding – Overdue – ERS staff (from various branches) continues to meet with State and county employer agencies to determine/update what is included in compensation for ERS benefits; to provide information on reporting processes and computer requirements; etc. The results of these findings will probably require legislative changes for the definition of ERS eligible compensation.</p> <p>ERS Work Report staff continues to utilize excel formulas and SQL queries to help analyze data files received and provide feedback to employers. Staff training is ongoing as</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
				<p>changes are made to the data files received.</p> <p>KMH LLP was contracted to assist ERS with internal compliance testing of employers' payroll and personnel reporting. Accounting and RBB are currently working with KMH on the audit criteria and procedures to review payroll reporting from employers for compliance with Act 87 requirements that are effective in July 2024.</p> <p>It is unrealistic to determine the final implementation date given the results are highly dependent on employers implementing changes to the payroll and personnel systems to accurately and consistently report information to ERS; or for ERS to modify its pension system. These systems require approval of funding</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
				from legislature and city councils.
Human Resources – Personnel Development and Retention Review				
<p>Finding 2 – The ERS can improve its succession planning processes by incorporating “Succession Management” into their plans.</p>	<p>IA recommends the ERS incorporate Succession Management into their existing succession planning processes. Key components of a succession management approach should include:</p> <ol style="list-style-type: none"> 1) Improved documentation around preparation, planning, and development improvement steps 2) Detailed developmental planning (training, coaching and mentoring) 3) Knowledge transfer and management practices 	Medium	<p>December 2021 (Revised #1 Target Date: December 2022) (Revised #2 Target Date: December 2023) (Revised #3 Target Date: March 2024) (Revised #4 Target Date: December 2024) (Revised #4 Target Date: June 2025)</p>	<p>Outstanding – Overdue – For Succession Management, each Branch Chief will identify the necessary skills/experience/knowledge required for those identified as their potential successors and improve documentation around developmental planning, etc.</p> <p>For the Accounting Branch, a succession plan has not been developed yet. The Accountant V position established in July 2023 was filled on October 1, 2024.</p>
Cloud Risk and Security Assessment - Phase 1 Review				
<p>Finding 1 – Identity, Credential, and Access Management controls have not been fully established to address cloud risk and security post implementation.</p>	<p>To reduce risks, we recommend the following:</p> <ol style="list-style-type: none"> 1. Establish user access policies, procedures, business processes, and technical measures for 	Medium	<p>September 2022 (Revised #1 Target Date: June 2024) (Revised #2 Target Date: TBD)</p>	<p>Outstanding – Extended Original Target Date – 1. - 1.3. Due to the significant number of vacancies in the I/S branch, Target Date is TBD for ERS</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>identity, entitlement, and access management.</p> <p>1.1. Establish a policy that documents access requirements, role-based access controls, and the IAM lifecycle for individuals accessing IT infrastructure i.e. the use of an access identity tool.</p> <p>1.2. Establish procedures that ensure provisioning of user access is authorized by the organization's management prior to access being granted, and is appropriately restricted as established in the policies and procedures.</p> <p>1.3. Establish procedures that ensure timely de-provisioning of user access to data, applications, infrastructure systems,</p>			<p>administrative governing policies and a schedule for the finalization of I/S policies will follow.</p> <p>1.4. Previously completed/responded to by I/S.</p> <p>2. The policy must first be developed in detail for these procedures (refer to response 1.0 of this section).</p> <p>3. Previously completed.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>and network components.</p> <p>1.4. Implement a federated identity management solution for on-premise and cloud environments to avoid the use of discrete accounts. Consider Azure Active Directory pass through authentication (PTA) for management of split on-premise and cloud authentication.</p> <p>2. Perform periodic user access reviews that verify that the organization is adhering to the rule of least privilege based on job function and that any terminated employees who have had access are removed. For any identified access violations, remediation must be performed and follow established user access policies and procedures.</p> <p>2.1. Verify user access to organization audit tools,</p>			



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>diagnostic and configuration ports, and utility programs capable of overriding the system is part of a periodic user access review.</p> <p>3. Evaluate access points of high risk (remote, privileged access) for implementation of multi-factor authentication requirements.</p>			
<p>Finding 2 – ERS has established patching policies and configuration hardening process to ensure that security vulnerabilities are addressed. However, enhancements are needed to ensure that these processes are matured for the cloud environment, especially for the hardening of Azure machine images and patching of Azure Linux systems.</p>	<p>We recommend the following to enhance and help establish patching procedures for workstations and servers:</p> <p>1. As ERS completes its Azure data center region change from Virginia to Arizona, work with Microsoft to understand their capabilities to assist with regular patching and vulnerability management. Establish an automated process to install vendor patches on at least a monthly basis for both installed applications and operating systems, including Linux.</p>	<p>Medium</p>	<p>September 2022 (Revised #1 Target Date: June 2024) (Revised #2 Target Date: TBD)</p>	<p>Outstanding – Extended Original Target Date – 1 and 2. Fiscal Year 2024, I/S branch procured Microsoft services to address these items. Pending vendor's response. 3. - 6. Due to the significant number of vacancies in the I/S branch, Target Date is TBD for ERS administrative governing policies and a schedule for the finalization of I/S policies will follow.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<ol style="list-style-type: none">1.1. Evaluate solutions to identify missing patches/vulnerabilities (vulnerability scanning). Consider Azure Defender for Servers.1.2. Evaluate solutions to deploy patches for the Azure environment, including Azure Automation Update Management.2. Implement or establish a threat intelligence function to monitor for newly announced vulnerabilities and released patches, and identify mitigating steps to fill the gap between the time a vulnerability is announced (known as '0-day') and the time a patch is provided by the vendor.3. Establish change control procedures that address emergency patching of critical resources, and various vulnerability scenarios must be created to ensure vulnerability			



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>remediation activities are properly documented and reviewed by technical teams prior to being mitigated, validated, and closed.</p> <p>4. Establish a formal risk management procedure to document unpatched vulnerabilities (e.g. risk acceptance sign-off by management), complete with tracking and periodic review.</p> <p>5. In coordination with the Office of Enterprise Technology Services, perform vulnerability scans of the internal and external networks of the production environment quarterly and non-production environment monthly to identify known vulnerabilities, missing patches, and misconfigurations.</p> <p>5.1. Implement a vulnerability management policy identifying timelines for patching based on risk level.</p>			



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>6. Evaluate usage of a hardened VM image from the Azure marketplace (e.g. CIS).</p> <p>After implementation is complete, management should establish procedures to monitor any changes to parameters or configurations that could lead to configuration drift.</p>			
<p>Finding 3 – Data Security policies are not in place to address the labeling, handling, and security of data and objects that contain data. Additionally, Encryption and Key Management policies and procedures are not fully established for the management of cryptographic keys in the service's cryptosystem.</p> <p>Finding 2 from IT Security Rapid Assessment & Internal Network Security Review (Outstanding – Overdue) – Management does not have</p>	<p>ERS should establish a data classification policy or procedure to identify types/classes of data and aid in handling data appropriately. The following should be incorporated into the data classification policy:</p> <ul style="list-style-type: none"> ▪ A definition of the types of data present in the ERS environment (e.g., PII, member data, sensitive/confidential). ▪ Data security requirements for each type of data. Requirements should be documented and maintained to give clear guidance on 	<p>Medium</p>	<p>September 2022 (Revised #1 Target Date: June 2024) (Revised #2 Target Date: TBD)</p>	<p>Outstanding – Extended Original Target Date – ERS initially started a data analytics group in 2023, but activity has been delayed due to other competing priorities. This group is led by the Chief Compliance Officer.</p> <p>Due to the significant number of vacancies in the I/S branch, Target Date is TBD for the finalization of I/S policies.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
<p>formal data classification policies and procedures in place to apply a risk-based approach towards handling, storing and transmitting of sensitive data other than personal information.</p>	<p>how to handle various data types (e.g., requirements for encryption, retention, handling, storage, transmission, destruction).</p> <ul style="list-style-type: none">Procedures should be documented for labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data. <p>Also establish an encryption and key management policy or procedure to ensure keys are appropriately secured, stored, and rotated, and additional key management activities are carried out. The following should be incorporated into the encryption and key management policy:</p> <ul style="list-style-type: none">Cryptographic keys, including TLS certificates, used to protect access to data and encrypt data at rest must be rotated periodically.			



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>Credentials and cryptographic keys must not be embedded or stored in source code or distributed in public facing repositories.</p>			
<p>Finding 4 – Logging and Monitoring procedures around security events, capacity resources, virtual machine integrity, and network traffic have not been fully defined. Additionally, a formal periodic review of logging configurations has not been established.</p>	<p>Logging and monitoring policies and procedures should be established and tools should be implemented. As ERS completes its Azure data center region change from Virginia to Arizona, the following areas should be considered when working with the vendor to implement logging and monitoring tools:</p> <ul style="list-style-type: none"> ▪ Any changes made to cloud instances must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts). 	<p>Medium</p>	<p>September 2022 (Revised #1 Target Date: June 2024) (Revised #2 Target Date: TBD)</p>	<p>Outstanding – Extended Original Target Date – ERS is working with a Virtual Chief Information Security Officer (vCISO). Due to the significant number of vacancies in the I/S branch, Target Date is TBD for implementation of SIEM / Managed Detection and Response (MDR) solution.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<ul style="list-style-type: none">▪ Capacity and necessary resources should be planned for, measured, and monitored to deliver the required system performance in accordance with ERS expectations.▪ Network environments and virtual instances should be designed and configured to restrict and monitor traffic between trusted and untrusted connections.▪ Centralize the use of logging solutions (Azure Log Analytics and SolarWinds) to better integrate and use the results. <p>Restrict the ERS Systems team's access to the audit logs appropriately (e.g., read-only).</p>			



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
<p>Finding 5 – Governance and risk management requirements for the cloud environment have not yet been established. Requirements should be established based on ERS risk profile and industry best practices. Once requirements are defined, compliance should be monitored on an ongoing (at least annual) basis.</p>	<p>Foundational governance and risk management requirements should be established to include the following:</p> <ul style="list-style-type: none"> ▪ Defining a Risk Management Policy that defines how ERS will identify, assess, track/monitor, remediate, and address risk. ▪ Regularly (at least annually) conducting a risk assessment. Utilize industry-standard sources like NIST 800-30 to guide assessment methodology. ▪ Document a remediation plan (such as a Plan of Action and Milestones – POA&M) to address identified risks. Regularly discuss with leadership on milestones and current risk register status. <p>In addition, we recommend ERS work with their vendors to find a mutually agreed upon external time source that is used to synchronize the system clocks of all relevant information</p>	<p>Low</p>	<p>September 2022 (Revised #1 Target Date: July 2024) (Revised #2 Target Date: TBD)</p>	<p>Outstanding – Extended Original Target Date – The I/S branch is still dealing with staff shortages. Due to the current staff shortages, ERS' priorities and current projects, this finding will be delayed. A new Target Date will be established once I/S has the resources to work on this. New Target Date is TBD.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>processing systems to facilitate tracing and reconstitution of activity timelines.</p> <p>We also recommend the IS branch work with the Procurement department to track data outages and determine thresholds where ERS may be eligible for financial compensation.</p>			
Employer Communication & Reporting Review				
<p>Finding 3 – Work report processing procedures are not detailed enough and do not capture the unique, detailed steps required when reviewing and processing reports for a specific employer agency. Work Reports Team staff are also not currently cross-trained to process and review an employer agency or department they are currently not assigned to.</p>	<p>IA recommends that each Work Reports Team staff have formal, consistent procedures, and sufficient detail to document how they address their assigned employer's issues and complexities in their review and processing of Work Reports.</p> <p>The Work Reports Team should develop a plan or schedule to ensure that the staff are able to cross train each other on their</p>	<p>Low</p>	<p>December 2023 (Revised #1 Target Date: December 2024) (Revised #1 Target Date: December 2025)</p>	<p>Outstanding – Extended Original Target Date – Revised Target Date is December 31, 2025 for the documented procedures.</p> <p>Cross training in Accounting's work report processing has occurred for several employer reports, although formalized procedures are still being worked on and revised by the team member who was</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	assigned employers and review files by using the procedures noted above.			<p>cross trained. Delays in documenting procedures have continued due to leaves, continued vacancy, and V3locity Migration Assessment.</p> <p>KMH LLP was contracted to assist ERS with internal compliance testing of employers' payroll and personnel reporting. Accounting and RBB are currently working with KMH on the audit criteria and procedures to review payroll reporting from employers for compliance with Act 87 requirements that are effective in July 2024.</p> <p>Further, there continues to be increased workload in payroll adjustments reported by employers (such as hazard pay, servicemen's act, salary adjustments and class code corrections). Accounting is also working with employers on implementing their system</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
				changes. Completing these objectives has been negatively impacted by the staff vacancy since October 2022.
Cloud Risk and Security Assessment – Phase 2				
<p>Finding 1 – Third-Party Risk Management ERS has not defined a process to assess and monitor third parties and vendors. Therefore, ERS does not perform periodic reassessments of third parties and vendors that have access to transmit or process the organization's data.</p>	<p>IA recommends that management address the finding in the following ways:</p> <ol style="list-style-type: none"> 1. Publish, finalize and disseminate the third-party risk management policy. Additionally, the policy should be reviewed at least annually. 2. Develop a formal third-party risk management program to provide critical insight into the effectiveness of third-party security controls. 	High	August 2024 (Revised #1 Target Date: TBD)	<p>Outstanding – Extended Original Target Date – Pending procurement of the Enterprise Risk Management, Audit, and Policy software by the Chief Compliance Officer, but activity has been delayed due to other competing priorities.</p> <ol style="list-style-type: none"> 1. Upon completion of procurement, I/S to work with ERS' Chief Compliance Officer, AG, and Administration to develop a third-party risk management policy. 2. Upon completion of procurement, I/S to work with ERS' Chief Compliance Officer to look into obtaining services to assist ERS in



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
				<p>developing a third-party risk management program as we do not have the expertise and/or resources necessary.</p> <p>Due to the significant number of vacancies in the I/S branch, Target Date is TBD for I/S.</p>
<p>Finding 2 – Threat and Vulnerability Management ERS has not defined a service-level agreement (SLA) for vulnerability patching. As a result, there may be high-risk vulnerabilities that are not patched in a timely manner. Our technical review of in-scope systems noted that patching was being conducted ad hoc and was not consistently performed on a monthly basis. Unpatched vulnerabilities can carry a significant risk and present attackers with additional time to exploit vulnerabilities.</p>	<p>IA recommends that management address the finding in the following ways:</p> <ol style="list-style-type: none"> 1. Define a vulnerability SLA for vulnerability patching for all known vulnerabilities based on achievability and the organization's risk appetite. 2. Continue to work with Microsoft to conduct an Azure penetration test, and remediate any vulnerabilities identified in a timely manner. Additionally, perform penetration tests at least annually, or upon significant changes to any public-facing connectivity channels. 	<p>High</p>	<p>June 2023, December 2023 (Revised #1 Target Dates: June 2023, December 2023, and December 2024) (Revised #2 Target Dates: December 2024 and TBD) (Revised #3 Target Date: December 2025) (Revised #4 Target Date: TBD)</p>	<p>Outstanding – Overdue –</p> <ol style="list-style-type: none"> 1. ERS is working with a Virtual Chief Information Security Officer (vCISO). Due to the significant number of vacancies in the I/S branch, Target Date is TBD. 2. It is ERS' goal to perform annual penetration tests. ERS completed a Cybersecurity Operations Security Test in April 2023, as the penetration test was not an option due to resources, costs and procurement. Due to the significant number of vacancies in the I/S branch, the ETA to complete a penetration test is December



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	3. Document, develop, and deploy a golden image for Windows servers to ensure that the operating system is hardened and baseline controls are implemented.			31, 2025, this date is subject to change. 3. Fiscal Year 2024, I/S branch procured Microsoft services to address these items. Pending vendor's response.
Finding 3 – Logging and Monitoring ERS utilizes Azure Log Analytics to collect logs for the Azure environment; however, ERS has not defined alerts or a regular log review process to identify and notify security personnel of potential threats.	IA recommends that management address the finding in the following ways: 1. Publish, finalize and disseminate the logging and monitoring policy. Additionally, review the data classification policy at least annually. 2. Develop a capital and resource plan to project future cloud capacity requirements as the organization continues to transition from on-premise to the cloud. Additionally, review this plan at least	High	December 2023, October 2023, and June 2024 (Revised #1 Target Date: June 2024 and TBD) (Revised #2 Target Date: TBD)	Outstanding – Extended Original Target Date – 1. This task is assigned to the Chief Compliance Officer, who is in the process of procuring a data classification application software. He will work in collaboration with the I/S branch to implement and manage. 2. - 4. Fiscal Year 2024, I/S branch procured Microsoft services to address these items. Pending vendor's response. Due to the significant number of



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>annually or upon any changes.</p> <ol style="list-style-type: none">3. Configure Azure Monitor to alert security personnel based on defined metrics indicating risks beyond an established threshold.4. Any changes made to cloud instances should generate an alert regardless of the running state (e.g., dormant, off or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to members through electronic methods (e.g., portals or alerts).5. Use an Azure NSG to filter network traffic between Azure resources in an Azure virtual network. NSGs should not be open to all IP address ranges, as this is not best practice. ERS should set the appropriate			<p>vacancies in the I/S branch. Target Date is TBD for implementation.</p> <p>5. Fiscal Year 2024, I/S branch procured Networking services to Monitor and Detect. I/S branch will need to work with ETS and vendor to address. Due to the significant number of vacancies in the I/S branch. Target Date is TBD for implementation.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>inbound rules. Also, enable Traffic Analytics. Traffic Analytics is an Azure-native solution that enables clients to receive insights about the Azure virtual network flows.</p>			
<p>Finding 4 – Identity and Access Management Procedures and controls surrounding user access have been established for ensuring appropriate identity, entitlement and access management of all users with access to data and application interfaces; however, these procedures have not been finalized, published or disseminated, and user access reviews are not being conducted on a periodic basis. Additionally, an on-premises domain controller is utilized, and a contingency plan has not been evaluated to allow uninterrupted user access in the case of a natural disaster. Lastly, storage accounts have not been configured to restrict access</p>	<p>IA recommends that management address the finding in the following ways:</p> <ol style="list-style-type: none"> 1. Publish, finalize and disseminate the identity and access management policy. Additionally, the policy should be reviewed at least annually. 2. Implement semiannual access reviews to ensure that all access is appropriate and access that is no longer needed is removed. Additionally, review user access when users resign, are terminated, change roles and/or no longer need the authorization to carry out duties for any other reason. 	<p>High</p>	<p>June 2023, September 2023, and June 2024 (Revised #1 Target Date: June 2024 and TBD) (Revised Date #2 Target Date: TBD)</p>	<p>Outstanding – Extended Original Target Date – Due to the recent staff turnover and current vacancies in the I/S branch, this has been put on hold. Target Date is TBD.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>3. Consider moving from Active Directory to Azure Active Directory to provide continuous availability in the event of equipment failure.</p> <p>4. Ensure that storage accounts restrict network access using virtual network rules and set up a private link connection for your storage accounts. Additionally, ensure that data is durable in the case of a complete regional outage or a disaster in which the primary region is not recoverable.</p>			



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
<p>Finding 5 – Data Security and Privacy Life Cycle Management Although ERS maintains a comprehensive backup strategy for Azure cloud, ERS has yet to fully operationalize data security and privacy life cycle management controls, resulting in a lack of data understanding and ownership and indicators of encryption and data security weaknesses.</p>	<p>IA recommends that management address the finding in the following ways:</p> <ol style="list-style-type: none"> 1. Publish, finalize and disseminate the data classification policy. Additionally, the policy should be reviewed at least annually. 2. Establish an encryption and key management policy or procedure to ensure that keys are appropriately secured, stored and rotated, and additional key management activities are carried out. 3. Update network and data flow diagrams annually or upon any changes to the environment that would impact such diagrams to ensure that they are current and up to date. 4. As ERS continues to migrate servers that are still on-premises over to Azure cloud, a data responsibility matrix should be developed to define data owners and 	<p>Medium</p>	<p>September 2023 and June 2025 (Revised #1 Target Date: June 2025 and TBD)</p>	<p>Outstanding – Extended Original Target Date –</p> <ol style="list-style-type: none"> 1. I/S will work with the ERS Chief Compliance Officer, Administration, procurement and AG to finalize and disseminate the data classification policy. Estimated completion date: June 30, 2025 2., 3., 5., and 6. Due to the recent staff turnover and current vacancies in the I/S branch, this has been put on hold. Target Date is TBD. 4. I/S will work with the ERS Chief Compliance Officer, Branch Chiefs & Administration to develop a data responsibility matrix. Estimated completion date: June 30, 2025 <p>Items 1 & 4 may be delayed until the compliance software is procured and vacant positions are filled.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>the data records for which they are responsible for.</p> <ol style="list-style-type: none"> 5. Enable “Adaptive application controls for defining safe applications” on the virtual machines. 6. ERS should enable Purge Protection and Soft Delete. Purge Protection and Soft Delete are features that safeguard against losing key access. 			
Member Enrollment & Re-Enrollment Process Review				
<p>Finding 1 – There is a shortage of SSS staffing and technology resources and lack of policies and procedures, resulting in a backlog of member enrollment forms, including ERS-1 and ERS Form 1A forms, that have not been imaged and indexed into the PAS. This backlog extends as far back to members who were enrolled over 12 months prior.</p>	<p>IA recommends that management address the above finding in the following ways:</p> <ol style="list-style-type: none"> 1. Develop well-documented policies and procedures for imaging and indexing documents into the PAS. 2. Update position descriptions for Office Assistants I and II to include document imaging and indexing and provide training. 3. Reduce the current backlog of enrollment form imaging 	High	<p>April 2025 (Latest Completion Date) (Revised Date #1 Target Date: June 2025)</p>	<p>Outstanding – Not Overdue –</p> <p>A procedure for imaging and indexing was created in October 2024.</p> <p>Two new scanners have been installed and now SSS has 3 working scanners (2 new ones and the legacy scanner) SSS has also been able to acquire (2) 89 day hires (one part time and one full-time). This has greatly</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>by assigning more internal staff resources to assist with imaging into the PAS.</p> <p>4. Procure an additional specialized scanner that is compatible with the PAS.</p>			<p>helped ease the tension and pressure of the current work load on current staff. SSS is still seeking permanent employees. When the 89 day hire contracts expire the backlog will continue as the section will revert back to the 62.5% staffing level with the same amount of current workload.</p> <p>All of the positions in SSS have been upgraded to OA III and OA IV positions. This implementation occurred sometime in 2023. Training is being provided. Re-describing the job descriptions of the OA III and OA IV positions are ongoing. Target Date: June 2025</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
<p>Finding 2 – A lack of file management policies and procedures resulted in significant delays in the ERS locating and providing requested enrollment forms. Management was unable to provide one or more enrollment forms for approximately 40% of the members requested.</p>	<p>IA recommends that management address the above finding in the following ways:</p> <ol style="list-style-type: none"> 1. Consult with the State of Hawaii Records Management Branch to determine an efficient and effective process and controls to manage ERS' records. 2. Develop well-documented policies and procedures for file management, organization and storage. These should include the file management process designed after consulting with the State of Hawaii Records Management Branch. 	High	June 2025 (Latest Completion Date)	<p>Outstanding – Not Overdue –</p> <p>1. The CCO is in the process of developing a records file management, organization, storage, retention and disposal policy in compliance with State of Hawaii records management policy. Target Date: June 2025</p> <p>2. SSS, IT, RBB and the CCO will work on the development of policies and procedures that address file management, organization and storage. Target Date: June 2025</p> <p>3. New high capacity scanners were acquired and installed in January 2025.</p>
<p>Finding 3 – Management does not have data integrity control activities in place to review and verify member enrollment data information input into the PAS, exposing the ERS to an increased risk of not detecting data input errors.</p>	<p>IA recommends that management implement the following to address this finding: RBB should develop a formal, documented review process to verify the accuracy of member enrollment information input into the PAS.</p>	Medium	<p>December 2024 (Revised #1 Target Date: March 2025) (Revised #2 Target Date: November 2025)</p>	<p>Outstanding – Extended Original Target Date –</p> <p>1. Go live pushed back. Working on Block 14 and will need Block 15 to process 2024 PIF files. New Target date: Fall 2025.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<ul style="list-style-type: none"> RBB should perform, at a minimum, a periodic review on a sample basis (i.e., weekly/bi-monthly review of a sample of new and return to work members). The reviewer should document the list of members reviewed, noting any errors identified, confirming that the review was completed and errors communicated with the RBB Office Assistant for correction and follow up. 			2. Pending. Program Specialists assigned as lead for this project.
<p>Finding 4 – Management does not have a control activity in place to verify that access to ERS' active directory and applications are properly disabled for all terminated employees, resulting in terminated employees inappropriately listed as current users per the PAS user access report.</p>	<p>IA recommends that management address the above finding by:</p> <ol style="list-style-type: none"> Implementing a formally documented, periodic (i.e. quarterly, semi-annually, annually) terminated user access review of active directory and applications, specifically the PAS, to detect terminated employees that may have access to a system/application. Developing an employee termination workflow process 	Medium	December 2024	<p>Cleared – Completed. Offboarding workflow was completed in December and it has been used. Based on feedback after using the workflow, we are working on the next revision which should be completed in March 2025.</p>



Issued Reports Finding Status (continued)

FINDING	RECOMMENDATION	RATING	TARGET COMPLETION DATE(S)	STATUS – PROVIDED BY MANAGEMENT
	<p>when the help desk system goes live with steps to disable/remove access to all systems and applications. Employee access should be fully disabled immediately upon termination.</p>			
<p>Finding 5 – There are currently no documented policies and procedures or any control activities in place to validate the Return to Work Transfers Log's completeness and accuracy, resulting in an incomplete listing of return to work members on the Return to Work Transfers Log.</p>	<p>IA recommends that management address the above finding in the following ways:</p> <ol style="list-style-type: none"> 1. Develop well-documented policies and procedures for updating and validating the completeness and accuracy of the Return to Work Transfers Log. 2. Periodically reconciling the Return to Work Transfers Log with a PAS report of return to work members to verify completeness and accuracy of the log. 	<p>Medium</p>	<p>November 2024, February 2025 (Revised #1 Target Date: November 2025) (Revised #1 Target Date: December 2025)</p>	<p>Outstanding – Extended Original Target Date –</p> <ol style="list-style-type: none"> 1. Update to completion: December 2025 2. Still pending completion in February 2025; dependent on IS & RBB schedules 3. Due to end of year retirements and need for all membership staff to assist, updating completion date to March 2025. Reviews are still being handled using interim process. 5. Still pending completion with target date of February 2025.



Appendix A: Virtual Chief Information Security Officer (vCISO) Bio



Ty Smith

Director, Office of the
CISO

Summary of experience

Ty is an experienced management consultant and U.S. Army officer, who has a strong understanding of information security within the professional services industry. He assists clients with executive management decisions surrounding information security to help ensure the highest return on investment. Ty has worked with organizations across a variety of industries, providing him with the experience and knowledge of the different ways that each industry secures its data. Ty also serves as a battalion communications officer in the Ohio National Guard.

Ty's professional experience serving as vCISO for multiple organizations over the past 7 years includes the third largest Children's hospital in the U.S., a large behavioral health system, several private equity funds, and a manufacturing carve-out. In his experience, Ty has helped organizations mature their cybersecurity programs, make strategic decisions, and educate executives/boards on cybersecurity issues.

Professional affiliations and credentials

- Masters of Business Administration, Auburn University
- Graduate Certificate, Management Information Systems, Auburn University
- Certified Information Systems Security Professional (CISSP)
- Certified vCISO
- Six Sigma Lean professional
- Active secret security clearance, Department of Defense

Risk Assessment Re-Evaluation and Proposed Two-Year Internal Audit Plan (January 1, 2025 – December 31, 2026)








Employees' Retirement System of the State of Hawaii

CONFIDENTIAL

This report is prepared solely for the internal use of the Employees' Retirement System management, the Administrative & Audit Committee, and the Board of Trustees. Distribution requires prior approval from the Administrative & Audit Committee or management

Table of Contents

	<u>Page</u>
 Executive Summary	3
 Risk Assessment Re-Evaluation Process	5
 Proposed Two-Year Internal Audit Plan	22
 Proposed Two-Year Internal Audit Plan Schedule	33
 Appendices	36

Executive Summary

Executive Summary

This report presents the results of Internal Audit’s (“IA”) Risk Assessment Re-Evaluation and the proposed Two-Year Internal Audit Plan for the State of Hawaii Employees’ Retirement System (“ERS”) for the periods from January 1, 2025 through December 31, 2025 and January 1, 2026 through December 31, 2026, collectively the “Audit Plan.”

The Audit Plan was developed based on the results of the risk assessment re-evaluation, which included revisiting the previous Risk Assessment and Audit Plan and interviews with members of management, the Board of Trustees (“Board”), and other associated parties. Risks were re-evaluated given changes within the industry and regulatory environment, internal organizational changes, results of completed IA reviews, our knowledge of the ERS’ business risks, and a high-level evaluation of the current internal control environment.

As a result of the Risk Assessment, 22 auditable areas for the ERS were deemed high risk and 25 were deemed medium risk. While these “high” and “medium” risk areas would justify a significant Internal Audit effort, current resources available to address these risks are limited. Therefore, IA is proposing 6 projects in 2025 and 5 projects in 2026. These projects are being proposed to address the higher risk areas, risk areas that are considered time sensitive or provide a larger coverage, as well as projects required in accordance with the Global Internal Audit Standards of the Institute of Internal Auditors (“IIA”).

The table below summarizes the hours for the Audit Plan, and a historical review of actual and projected hours compared to the budget for the past two years, 2023 and 2024. As risks to the ERS change over time, management and the Administrative & Audit Committee are encouraged to re-evaluate the Internal Audit Plan.

Internal Audit Activity Hours						
	2023		2024		2025	2026
	2/1/23 - 12/31/23		1/1/24 - 12/31/24		1/1/25 - 12/31/25	1/1/26 - 12/31/26
	Budgeted	Actual	Budgeted	Actual	Proposed	Proposed
Carryover Projects	-	-	285	302	525	-
Assurance	1,000	322	1,100	615	1,000	1,700
Advisory & Other	1,575	1,336	1,650	1,019	2,250	1,300
Total	2,575	1,658	3,035	1,936	3,775	3,000

Risk Assessment Re-Evaluation Process

Risk Assessment Re-Evaluation Process – Overview

Our update process began with the results of the previous Risk Assessment Re-Evaluation conducted in 2023. Risks were re-evaluated based on any changes to the ERS' internal and external environments as well as results of audits completed over the past year. The following is a summary of our re-evaluation process.



AUDIT UNIVERSE

Understand Changes to the ERS' Audit Universe

- Identify new and/or changes to the ERS' auditable areas
- Validate the population is current, well defined, appropriate, and complete



RISK IDENTIFICATION

Identify Key Risks, Concerns & Issues

- Analyze industry changes and current internal and external environments
- Identify new and emerging risks relevant to the ERS
- Work with Senior Management and Board of Trustees to update understanding of ERS' key risks



RISK EVALUATION & RISK MAPPING

Prioritize Key Risks, Concerns & Issues Identified

- Re-assess inherent risks for each auditable area
- Re-evaluate residual risk factors to develop composite risk score
- Re-rank each auditable area by risk score
- Select high-risk/high-importance auditable areas



AUDIT PLAN DEVELOPMENT

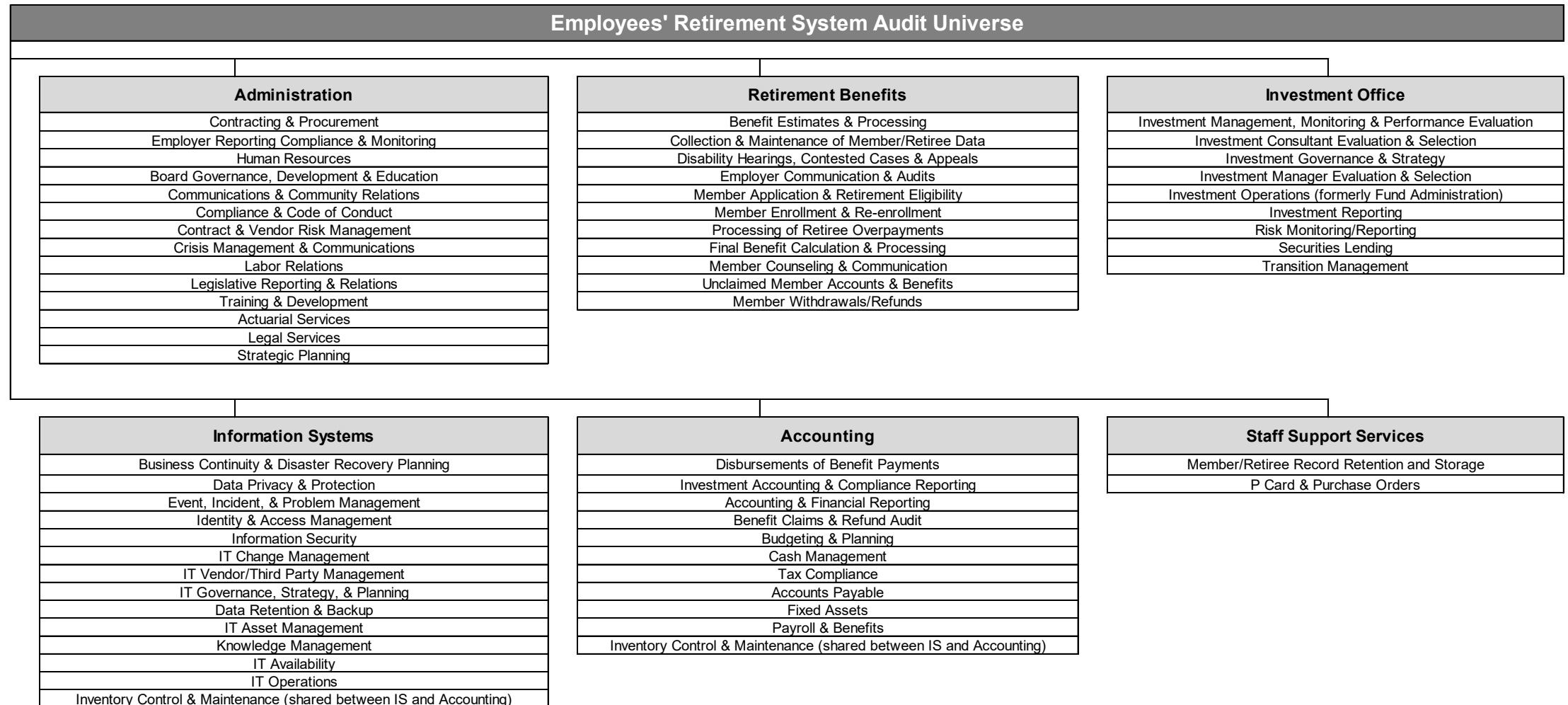
Create Responsive Internal Audit Plan

- Re-focus the Audit Plan on the key control processes and high risk auditable areas
- Develop a balanced Audit Plan comprised of financial, operational and compliance audits, and where applicable, special projects
- Ensure audit coverage of significant risk areas

By developing an understanding of the key risks and issues at the ERS, IA developed a focused plan, which will coordinate management, internal audit and external audit resources to ensure maximum risk coverage.

Risk Assessment Re-Evaluation Process – Audit Universe

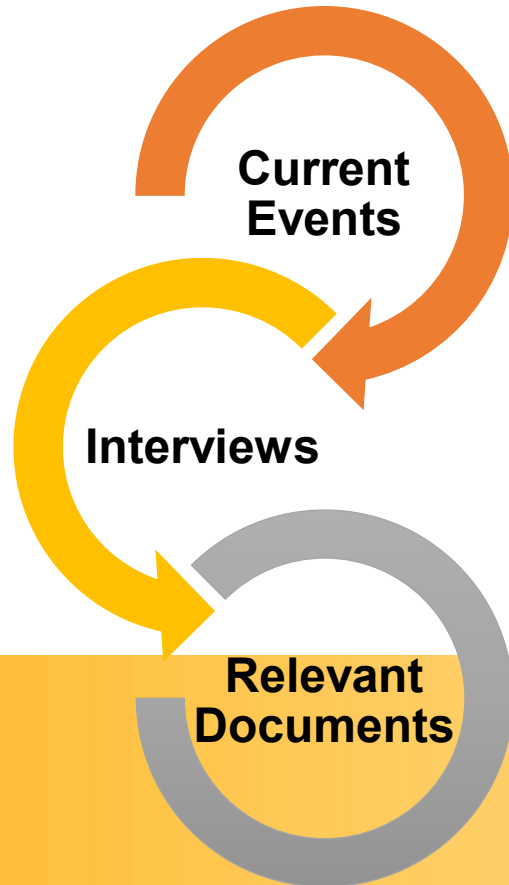
For the update to the Audit Universe, IA validated that the population of **auditable areas** was well defined, appropriate, current, and complete. This validation was accomplished based primarily on interviews with key management personnel. The Audit Universe for the ERS is detailed below.



Risk Assessment Re-Evaluation Process – Risk Identification

After finalizing updates to the Audit Universe, IA confirmed and identified relevant risks to the ERS during the Risk Identification phase and performed the following steps:

- Obtained an understanding of current events impacting the ERS.
- Interviewed members of management, the Board, and external auditor.
- Reviewed relevant reports and documents.



Understanding of Current Events – Based on discussions and review of relevant documents, the following are a few of the more significant current events:

- Implementation of a new pension administration system, V3locity, to begin in calendar year 2025.
- Hiring of a new Deputy Executive Director to lead and oversee branch operations.
- Increased focus on strategic planning and succession in preparation for ERS’ future.

Conducted Interviews – Please see **Appendix A** for a complete list of individuals that were interviewed.

Reviewed Relevant Documents – IA reviewed a variety of significant reports and documents that were prepared by management or issued by consultants including, but not limited to: Strategic Plan, External Financial Audit and Actuarial Valuation Reports, Policies & Procedures, Investment Reports, and Internal Metrics.

Risk Assessment Re-Evaluation Process – Risk Identification

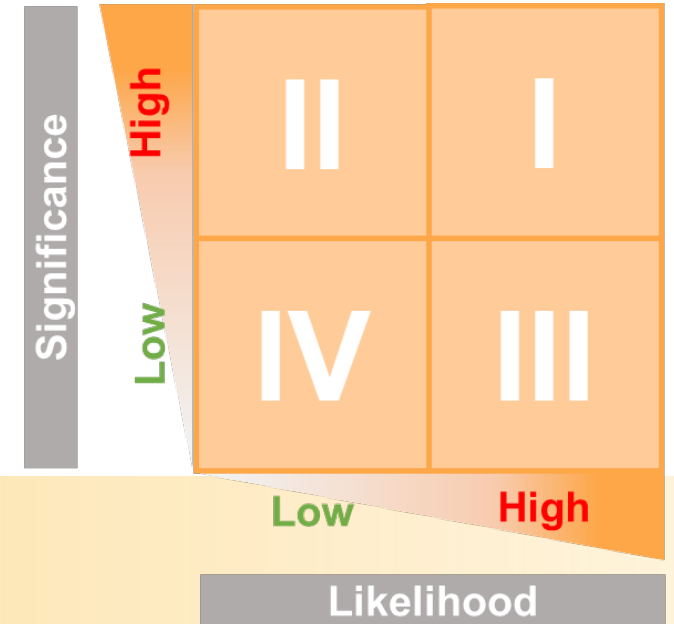
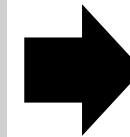
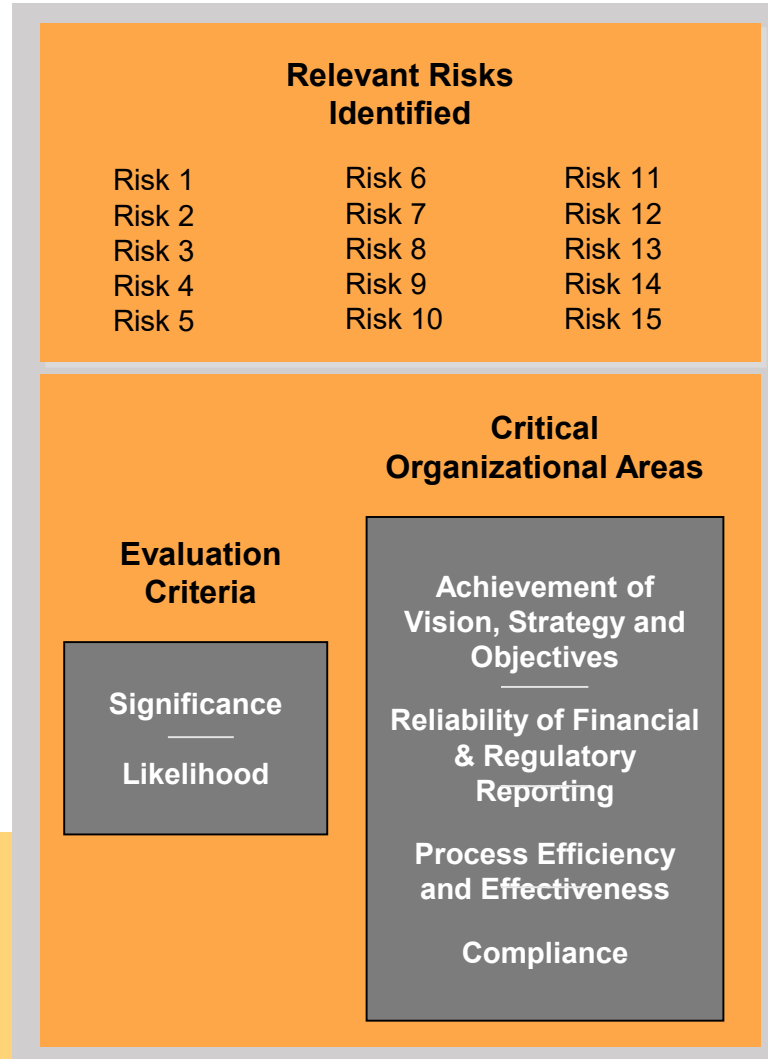
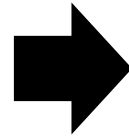
A component of the Risk Identification phase was an identification of relevant risks utilizing an Enterprise-wide Risk Model representing the universe of possible risks. The following is the listing of risks classified into three major areas of *Environment Risks*, *Process Risks* and *Information for Decision-Making Risks*. Certain risks within the Risk Model were not applicable, and others were modified to better fit the ERS as deemed necessary. A description of all relevant risks are defined in more detail in **Appendix B** and **C**.

ENVIRONMENT RISK	PROCESS RISK			INFORMATION FOR DECISION-MAKING RISK
<ul style="list-style-type: none"> Competitor Customer Wants Technological Innovation Sensitivity Shareholder Expectations Capital Availability Sovereign/Political Legal Regulatory/Legislative Industry Financial Markets Catastrophic Loss 	<p><u>FINANCIAL</u></p> <p>Price Interest Rate Currency Equity Commodity Financial Instrument</p>	<p><u>EMPOWERMENT</u></p> <p>Leadership Authority/Limit Outsourcing Performance Incentives Change Readiness Communications</p>	<p><u>GOVERNANCE</u></p> <p>Organizational Culture Ethical Behavior Board Effectiveness Succession Planning</p>	<p><u>STRATEGIC</u></p> <p>Environmental Scan Business Model Portfolio Investment Valuation/Evaluation Organization Structure Measurement (Strategy) Resource Allocation Planning Life Cycle</p>
	<p>Liquidity Cash Flow Opportunity Cost Concentration</p>	<p><u>INFORMATION TECHNOLOGY</u></p> <p>Integrity Access Availability Infrastructure Security</p>	<p><u>REPUTATION</u></p> <p>Image and Branding Privacy Stakeholder Relations</p>	<p><u>PUBLIC REPORTING</u></p> <p>Financial Reporting Evaluation Internal Control Evaluation Executive Certification Taxation Pension Fund Regulatory Reporting</p>
	<p>Credit Default Concentration Settlement Capital/Collateral</p>		<p><u>INTEGRITY</u></p> <p>Management Fraud Employee Fraud Third Party Fraud Illegal Acts Unauthorized Use</p>	<p><u>OPERATIONAL</u></p> <p>Budget and Planning Product/Service Pricing Contract Commitment Measurement (Operations) Alignment Accounting Information</p>
	<p><u>OPERATIONS</u></p> <p>Customer Satisfaction Human Resources Knowledge Capital Product Development Efficiency Capacity</p>	<p>Scalability Performance Gap Cycle Time Sourcing Channel Effectiveness Partnering</p>	<p>Compliance Business Interruption Service Failure Environmental Health and Safety Trademark/Brand Erosion</p>	

Risk Assessment Re-Evaluation Process – Risk Identification

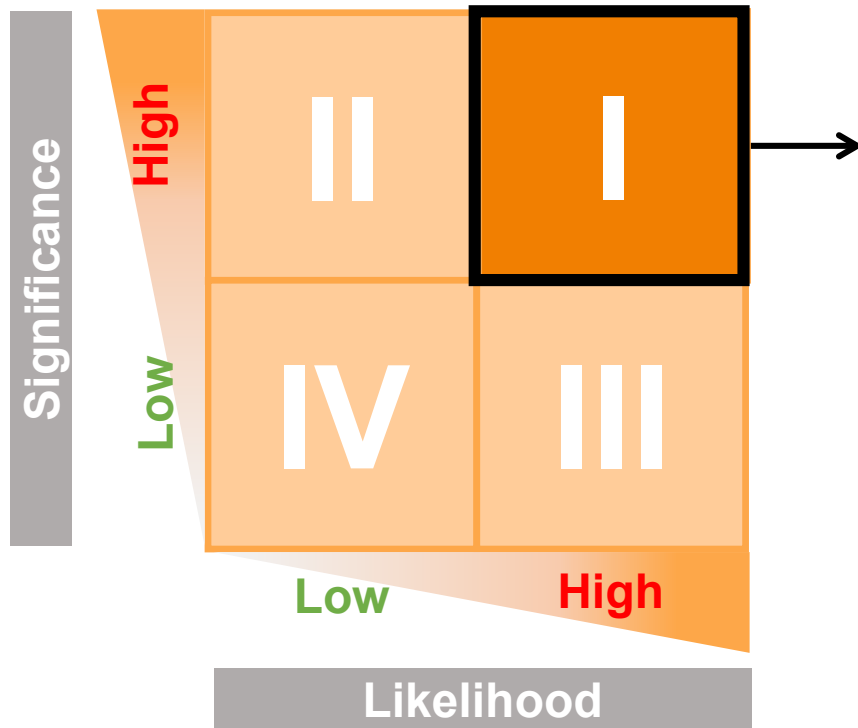
After identifying the relevant risks to the ERS, the relevant risks were assessed for *significance* and *likelihood* of an occurrence to negatively impact the *critical organizational areas* of the ERS. The high risks (Quadrant I) were identified and are listed on page 11.

ENVIRONMENT RISK	PROCESS RISK			INFORMATION FOR DECISION-MAKING RISK
<ul style="list-style-type: none"> Competitor Customer Wants Technological Innovation Sensitivity Shareholder Expectations Capital Availability Sovereign/Political Legal Regulatory/Legislative Industry Financial Markets Catastrophic Loss 	FINANCIAL <ul style="list-style-type: none"> Price Interest Rate Currency Equity Commodity Financial Instrument 	EMPOWERMENT <ul style="list-style-type: none"> Leadership Authority/Limit Outsourcing Performance Incentives Change Readiness Communications 	GOVERNANCE <ul style="list-style-type: none"> Organizational Culture Ethical Behavior Board Effectiveness Succession Planning 	STRATEGIC <ul style="list-style-type: none"> Environmental Scan Business Model Portfolio Investment Valuation/Evaluation Organization Structure Measurement (Strategy) Resource Allocation Planning Life Cycle
	Liquidity <ul style="list-style-type: none"> Cash Flow Opportunity Cost Concentration 	INFORMATION TECHNOLOGY <ul style="list-style-type: none"> Integrity Access Availability Infrastructure Security 	REPUTATION <ul style="list-style-type: none"> Image and Branding Privacy Stakeholder Relations 	PUBLIC REPORTING <ul style="list-style-type: none"> Financial Reporting Evaluation Internal Control Evaluation Executive Certification Taxation Pension Fund Regulatory Reporting
	Credit <ul style="list-style-type: none"> Default Concentration Settlement Capital/Collateral 	OPERATIONS <ul style="list-style-type: none"> Scalability Performance Gap Cycle Time Sourcing Channel Effectiveness Partnering 	INTEGRITY <ul style="list-style-type: none"> Management Fraud Employee Fraud Third Party Fraud Illegal Acts Unauthorized Use 	OPERATIONAL <ul style="list-style-type: none"> Budget and Planning Product/Service Pricing Contract Commitment Measurement (Operations) Alignment Accounting Information
	<ul style="list-style-type: none"> Customer Satisfaction Human Resources Knowledge Capital Product Development Efficiency Capacity 	<ul style="list-style-type: none"> Compliance Business Interruption Service Failure Environmental Health and Safety Trademark/Brand Erosion 		



Risk Assessment Re-Evaluation Process – Risk Identification

The following represents the high significance/high likelihood risks (Quadrant I) identified for the ERS. Quadrant I risks are defined in detail in **Appendix B**. All other relevant risks in the three remaining Quadrants (II, III, and IV) are defined in **Appendix C**.



Quadrant I Risks

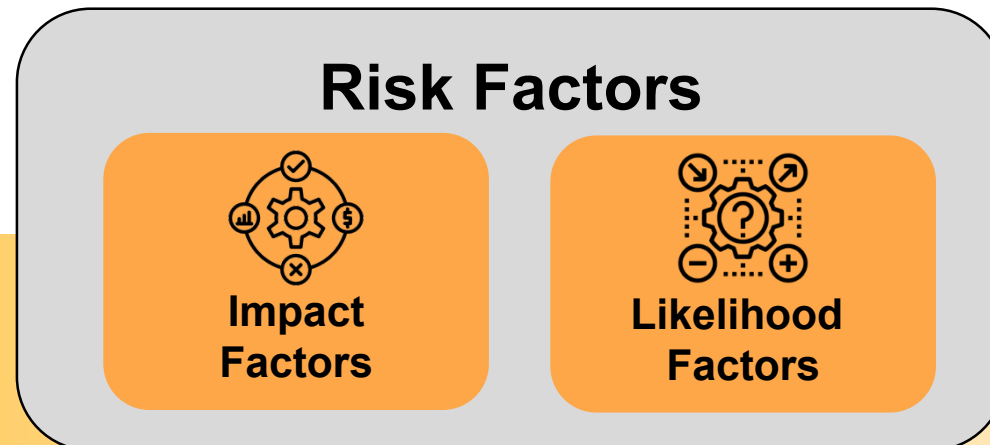
Access Risk	Infrastructure Risk
Accounting Information Risk	Knowledge Capital Risk
Alignment Risk	Leadership Risk
Business Interruption Risk	Organization Structure Risk
Capital Availability Risk	Organizational Culture Risk
Communications Risk	Performance Gap Risk
Compliance Risk	Privacy Risk
Contract Commitment Risk	Regulatory/Legislative Risk
Credit Risk	Resource Allocation Risk
Customer Satisfaction Risk	Security Risk
Cycle Time Risk	Service Failure Risk
Efficiency Risk	Succession Planning Risk
Financial Markets Risk	Technological Innovation Risk
Human Resources Risk	

Risk Assessment Re-Evaluation Process – Risk Evaluation

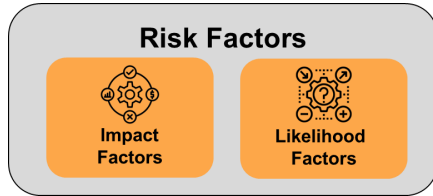
After identifying and assessing all relevant risks within the Enterprise-wide Risk Model, IA conducted a risk evaluation of the auditable areas using similar variables for the evaluation criteria.

The purpose of the Risk Evaluation phase was to determine the potential impact and likelihood of risks within each **auditable area**. IA utilized eight factors to score each **auditable area** as a *high*, *medium* or *low* risk. The final rankings of these **auditable areas** are summarized on page 15. The risks with the greatest adverse effect on the achievement of process and strategic level objectives deserve the most attention in the Audit Plan. In addition, any auditable area could be subject to an internal audit dependent on the risk related concerns of the ERS.

Risk is considered to be a function of 1) the **impact** to the ERS if a control weakness is successfully exploited, and 2) the **likelihood** that control weaknesses exist. Accordingly, IA scored risk for all auditable areas based on the following factors:



Risk Assessment Re-Evaluation Process – Risk Evaluation



Impact Factors: *Factors that dictate the degree to which the exploitation of a potential control weakness could harm the ERS:*

Financial

The maximum financial exposure (asset, revenue or expenses) that could be suffered. The following considerations were taken into account for this risk factor: liquidity of asset (degree to which assets can be readily converted to cash), ease of asset replacement and the relative financial impact on the ERS' budget or operational results.

Reputational Exposure

The greater the effect that an auditable area has on the ERS' Strategic Plan's goals and objectives, the greater the impact score.

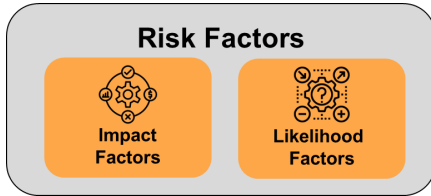
Compliance Exposure

The exposure to potential litigation and/or compliance with required laws, policies, standards, regulations and/or statutes.

Organizational Goals & Objectives

The greater the effect that an auditable area has on the ERS' Strategic Plan's goals and objectives, the greater the impact score.

Risk Assessment Re-Evaluation Process – Risk Evaluation



Likelihood Factors: *Factors that influence the probability that a potential control weakness exists:*

Transaction Volume

A higher transaction volume increases the likelihood that a control weakness will be exploited.

Previous Incidents or Findings

Previous incidents resulting from a control weakness or findings of a control weakness contained in previous audit, examination, or external consultant reports increase the likelihood of an existing control weakness.

Reliability & Integrity of Information System(s)

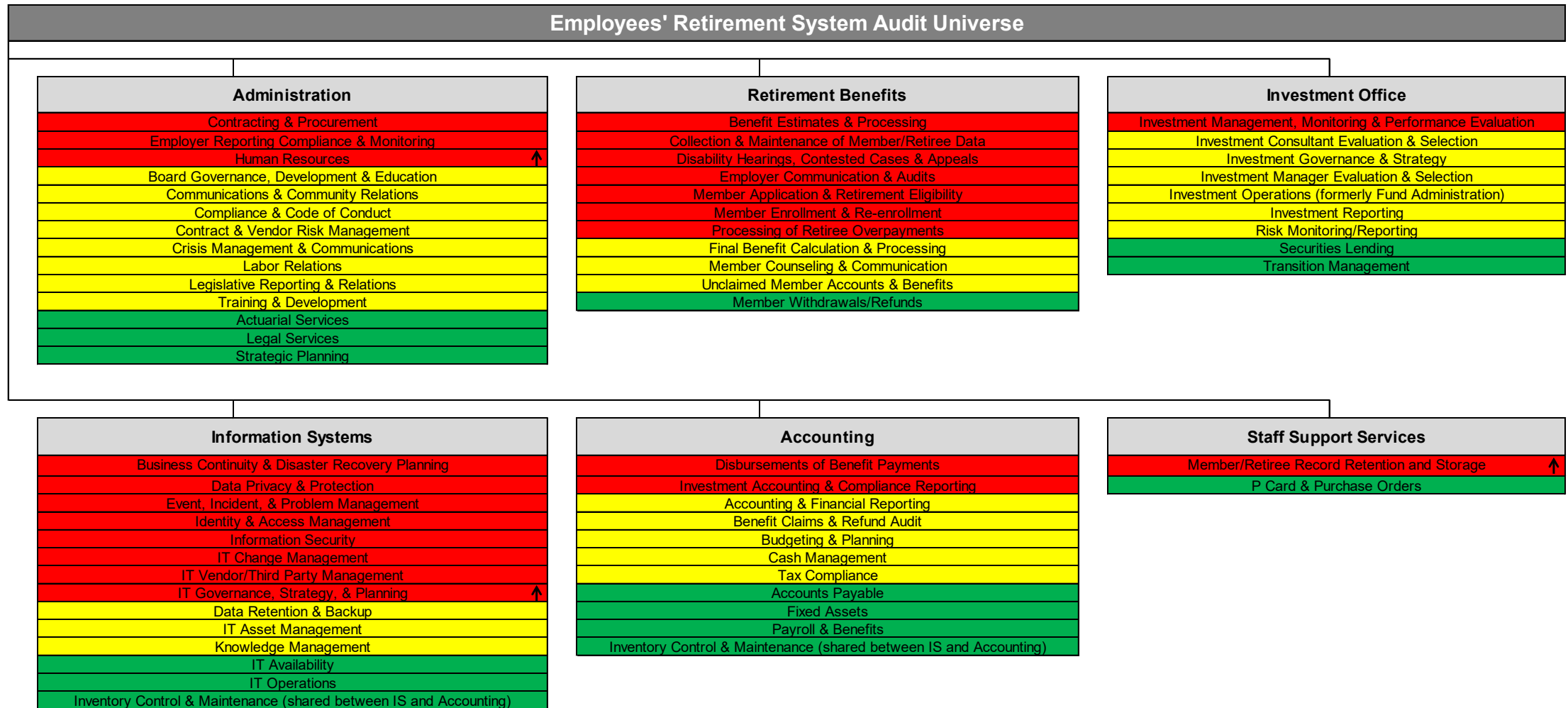
A measure of the level of reliability and integrity of the information system(s) used in the auditable area. The following considerations were taken into account for this risk factor: extent of system changes, automation or upgrades; disaster causing loss of systems, business interruption or destruction of data; technological obsolescence and documentation of system architecture; loss of data or access to data by unauthorized parties; operating environment complexity and organizational knowledge of application platform; degree of reliance on automated systems/outside vendors to process transactions; and strength of security access controls.

Process Complexity

Increased complexity raises the likelihood of a control weakness. The following considerations were taken into account for this risk factor: the number of workflow touch-points, manual calculations, sophisticated algorithms and multiple systems; departmental maturity was also considered, whereby the presence of seasoned staff may offset some of the effects of complex processes; extent of recent and planned changes in operations and reliance on vendors, consultants or specialists.

Risk Assessment Re-Evaluation Process – Risk Evaluation

After calculating the risk score for each auditable area, IA ranked them into high (red), medium (yellow) or low (green) risk areas. We have also indicated risk ratings that have changed since the 2023 Risk Assessment, ↑ indicating an increase in risk rating and ↓ indicating a decrease in risk rating.



Risk Assessment Re-Evaluation Process – Risk Evaluation

The following table represent the risk ratings by Branch for the ERS. Out of a total of 57 auditable areas, 22 are considered *high* risk. We have also indicated risk ratings that have changed since the 2023 Risk Assessment, indicating an ↑ increase in risk rating and ↓ indicating a decrease in risk rating.

Branch	Auditable Area	2023 Final Risk Rating	2024 Final Risk Rating	
Admin	Contracting & Procurement	High	High	
Admin	Employer Reporting Compliance & Monitoring	High	High	
Admin	Human Resources	Medium	High	↑
RBB	Benefit Estimates & Processing	High	High	
RBB	Collection & Maintenance of Member/Retiree Data	High	High	
RBB	Disability Hearings, Contested Cases & Appeals	High	High	
RBB	Employer Communication & Audits	High	High	
RBB	Member Application & Retirement Eligibility	High	High	
RBB	Member Enrollment & Re-enrollment	High	High	
RBB	Processing of Retiree Overpayments	High	High	
Investment	Investment Management, Monitoring & Performance Evaluation	High	High	
IS	Business Continuity & Disaster Recovery Planning	High	High	
IS	Data Privacy & Protection	High	High	
IS	Event, Incident, & Problem Management	High	High	
IS	Identity & Access Management	High	High	
IS	Information Security	High	High	
IS	IT Change Management	High	High	
IS	IT Vendor/Third Party Management	High	High	
IS	IT Governance, Strategy, & Planning	Medium	High	↑
Acctg	Disbursements of Benefit Payments	High	High	
Acctg	Investment Accounting & Compliance Reporting	High	High	
SSS	Member/Retiree Record Retention and Storage	Medium	High	↑

Risk Assessment Re-Evaluation Process – Risk Evaluation

The following tables represent the remaining risk ratings for the ERS. 25 auditable areas are considered *medium* risk.

Branch	Auditable Area	2023 Final Risk Rating	2024 Final Risk Rating
Admin	Board Governance, Development & Education	Medium	Medium
Admin	Communications & Community Relations	Medium	Medium
Admin	Compliance & Code of Conduct	Medium	Medium
Admin	Contract & Vendor Risk Management	Medium	Medium
Admin	Crisis Management & Communications	Medium	Medium
Admin	Labor Relations	Medium	Medium
Admin	Legislative Reporting & Relations	Medium	Medium
Admin	Training & Development	Medium	Medium
RBB	Final Benefit Calculation & Processing	Medium	Medium
RBB	Member Counseling & Communication	Medium	Medium
RBB	Unclaimed Member Accounts & Benefits	Medium	Medium
Investment	Investment Consultant Evaluation & Selection	Medium	Medium
Investment	Investment Governance & Strategy	Medium	Medium
Investment	Investment Manager Evaluation & Selection	Medium	Medium
Investment	Investment Operations (formerly Fund Administration)	Medium	Medium
Investment	Investment Reporting	Medium	Medium
Investment	Risk Monitoring/Reporting	Medium	Medium
IS	Data Retention & Backup	Medium	Medium
IS	IT Asset Management	Medium	Medium
IS	Knowledge Management	Medium	Medium
Acctg	Accounting & Financial Reporting	Medium	Medium
Acctg	Benefit Claims & Refund Audit	Medium	Medium
Acctg	Budgeting & Planning	Medium	Medium
Acctg	Cash Management	Medium	Medium
Acctg	Tax Compliance	Medium	Medium

Risk Assessment Re-Evaluation Process – Risk Evaluation

13 auditable areas are considered *low* risk.

Branch	Auditable Area	2023 Final Risk Rating	2024 Final Risk Rating
Admin	Actuarial Services	Low	Low
Admin	Legal Services	Low	Low
Admin	Strategic Planning	Low	Low
RBB	Member Withdrawals/Refunds	Low	Low
Investment	Securities Lending	Low	Low
Investment	Transition Management	Low	Low
IS	IT Availability	Low	Low
IS	IT Operations	Low	Low
IS/Acctg	Inventory Control & Maintenance (shared between IS and Accounting)	Low	Low
Acctg	Accounts Payable	Low	Low
Acctg	Fixed Assets	Low	Low
Acctg	Payroll & Benefits	Low	Low
SSS	P Card & Purchase Orders	Low	Low

Risk Assessment Re-Evaluation Process – Audit Plan Development

Finally, the auditable areas with the highest risk scores were linked to the high risks (Quadrant I) identified. The set of internal audit projects were determined by also considering factors such as the existence and maturity of key processes, balancing the risks at the ERS, and IA's resources available to perform the projects. Furthermore, in determining the timing of such projects, we considered (1) the impact on the various branches, as some branches are affected by multiple reviews/audit projects and (2) the efficient sequencing of projects that provide opportunities to leverage work performed and knowledge gained on preceding projects.

Branch	Auditable Area	2023 Final Risk Rating	2024 Final Risk Rating
Admin	Contracting & Procurement	High	High
Admin	Employer Reporting Compliance & Monitoring	High	High
Admin	Human Resources	Medium	High
RBB	Benefit Estimates & Processing	High	High
RBB	Collection & Maintenance of Member/Retiree Data	High	High
RBB	Disability Hearings, Contested Cases & Appeals	High	High
RBB	Employer Communication & Audits	High	High
RBB	Member Application & Retirement Eligibility	High	High
RBB	Member Enrollment & Re-enrollment	High	High
RBB	Processing of Retiree Overpayments	High	High
Investment	Investment Management, Monitoring & Performance Evaluation	High	High
IS	Business Continuity & Disaster Recovery Planning	High	High
IS	Data Privacy & Protection	High	High
IS	Event, Incident, & Problem Management	High	High
IS	Identity & Access Management	High	High
IS	Information Security	High	High
IS	IT Change Management	High	High
IS	IT Vendor/Third Party Management	High	High
IS	IT Governance, Strategy, & Planning	Medium	High
Acctg	Disbursements of Benefit Payments	High	High
Acctg	Investment Accounting & Compliance Reporting	High	High
SSS	Member/Retiree Record Retention and Storage	Medium	High

Branch	Auditable Area	2023 Final Risk Rating	2024 Final Risk Rating
Admin	Board Governance, Development & Education	Medium	Medium
Admin	Communications & Community Relations	Medium	Medium
Admin	Compliance & Code of Conduct	Medium	Medium
Admin	Contract & Vendor Risk Management	Medium	Medium
Admin	Crisis Management & Communications	Medium	Medium
Admin	Labor Relations	Medium	Medium
Admin	Legislative Reporting & Relations	Medium	Medium
Admin	Training & Development	Medium	Medium
RBB	Final Benefit Calculation & Processing	Medium	Medium
RBB	Member Counseling & Communication	Medium	Medium
RBB	Unclaimed Member Accounts & Benefits	Medium	Medium
Investment	Investment Consultant Evaluation & Selection	Medium	Medium
Investment	Investment Governance & Strategy	Medium	Medium
Investment	Investment Manager Evaluation & Selection	Medium	Medium
Investment	Investment Operations (formerly Fund Administration)	Medium	Medium
Investment	Investment Reporting	Medium	Medium
Investment	Risk Monitoring/Reporting	Medium	Medium
IS	Data Retention & Backup	Medium	Medium
IS	IT Asset Management	Medium	Medium
IS	Knowledge Management	Medium	Medium
Acctg	Accounting & Financial Reporting	Medium	Medium
Acctg	Benefit Claims & Refund Audit	Medium	Medium
Acctg	Budgeting & Planning	Medium	Medium
Acctg	Cash Management	Medium	Medium
Acctg	Tax Compliance	Medium	Medium



Quadrant I Risks

<ul style="list-style-type: none"> Access Risk Accounting Information Risk Alignment Risk Business Interruption Risk Capital Availability Risk Communications Risk Compliance Risk Contract Commitment Risk Credit Risk Customer Satisfaction Risk Cycle Time Risk Efficiency Risk Financial Markets Risk Human Resources Risk 	<ul style="list-style-type: none"> Infrastructure Risk Knowledge Capital Risk Leadership Risk Organization Structure Risk Organizational Culture Risk Performance Gap Risk Privacy Risk Regulatory/Legislative Risk Resource Allocation Risk Security Risk Service Failure Risk Succession Planning Risk Technological Innovation Risk
--	---

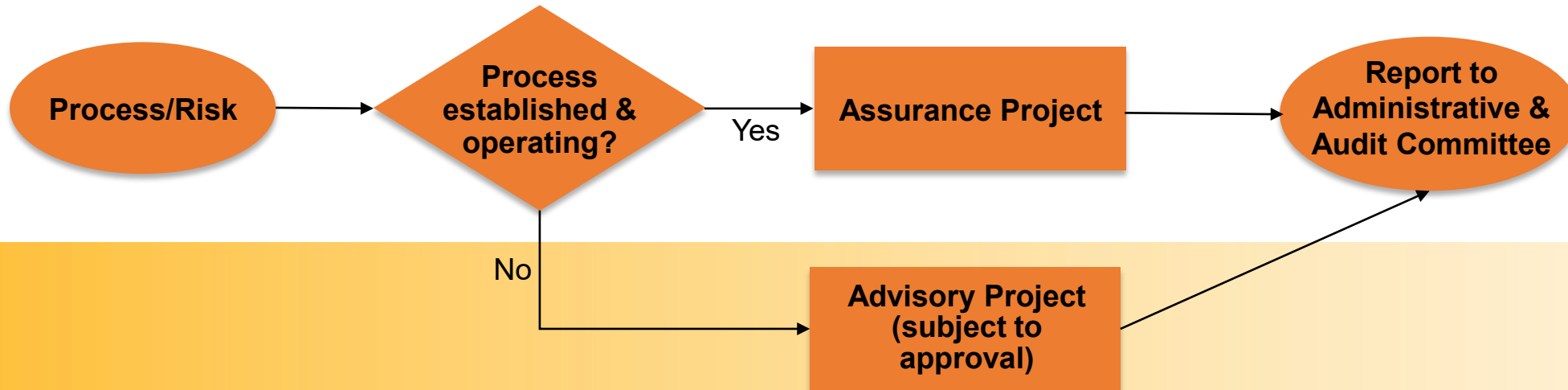


Internal Audit Plan – February 1, 2025 through December 31, 2025				
Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
2024 CARRYOVER PROJECTS				
Investment Manager Selection and Evaluation Review				
Project objectives include:				
<ul style="list-style-type: none"> • Evaluate the Investment Office's compliance with the requirements and internal controls set forth in the ERS' Investment Manager Selection Process Framework, which is comprised of stages to identify, evaluate, recommend, and approve prospective investment managers. • Assess whether the ERS' Investment Manager Selection Process Framework aligns with leading practices recommended by professional investment organizations and/or performed by peer pension systems in order to identify opportunities to enhance the current framework. • Provide recommendations and leading practices for improvements to enhance effectiveness and efficiency, where applicable. 	Investment Office <i>Investment Management Evaluation & Selection</i>	Authority/Limit Risk Alignment Risk Efficiency Risk Performance Gap Risk Service Failure Risk	Q1	150
<i>PRIMARY FOCUS: Operational/Financial</i>				

Risk Assessment Re-Evaluation Process – Audit Plan Development

The Audit Plan is focused primarily on evaluating and testing key control processes mitigating the “High” and “Medium” Auditable Areas and highly significant and likely risks (Quadrant I) impacting the ERS. The Audit Plan includes the following types of projects:

- **Assurance Projects:** *Established processes* are in place and will be evaluated for design and operating effectiveness. Executing the projects using IA’s methodology will require the performance of a **project-level risk assessment**, during which time significant and other additional relevant risks are evaluated and more detailed controls are identified to be considered for inclusion in the project scope.
- **Advisory Projects:** Processes under development or consideration by management may require **consulting** and related **client service activities**. The nature and scope of such projects are agreed upon with management and the Board, and are intended to add value and improve operations from a risk perspective. Advisory projects shall not in any circumstance impair IA’s independence.



Risk Assessment Re-Evaluation Process – Audit Plan Development

Based on the risk scores and risk ratings, IA identified 50+ projects (both assurance and consulting) that focus on addressing the high and medium risks and specific concerns raised within the ERS. However, due to the time and resource constraints, IA is proposing that the updated Audit Plan include **11 projects (listed in blue)** that are considered higher risk, time sensitive, an ERS priority, or provide a larger coverage, as well as those that are required in accordance with the standards of the IIA. Projects that have been previously completed or is in process are identified in **green**.

In addition, certain auditable areas do not currently have mature processes in place and as a result, IA chose not to include these areas within the Audit Plan at this time. IA will continue to monitor these areas and bring these risks to the attention of the Administrative & Audit Committee at the quarterly Administrative & Audit Committee presentations. The projects that did not make it to the Audit Plan have been established as a “Watchlist.” These projects will be monitored by IA and can be added to the Audit Plan should additional resources become available or at the request of the Administrative & Audit Committee.

Internal Audit Projects

Compliance & Code of Conduct
Communications & Community Relations Review
Human Resources - Personnel Development & Retention Review
Governance & Ethics Review
Business Continuity & Disaster Recovery Plan Planning
Business Continuity & Disaster Recovery Plan Training
Business Continuity Plan - Crisis Communication Plan Development
Employer Communication & Reporting Review
Business Continuity Plan - Tabletop Exercise
ERM Capability Roadmap and Training
Contracting & Procurement Review
V3locity Business Readiness Assessment
Strategic Planning Review
Budgeting Process Review
Legislative Reporting & Relations Review
Cash & Liquidity Management Review
Benefit Disbursement Review
Financial Reporting Process Review

Benefit Claims & Refund and Retiree Overpayments Processing Review
Investment Accounting Review
Records Management & Retention Review
Member/Retiree Record Processing, Retention, and Storage
Investment & Risk Monitoring & Reporting Review
Investment Governance Structure & Oversight Review
Investment Consultant Selection & Evaluation Review
Investment Management, Monitoring & Performance Evaluation Review
Investment Manager Selection & Evaluation Review
Continuous Monitoring Tool Development - Part 1
Continuous Monitoring Tool Development - Part 2
Continuous Monitoring Tool Development - Part 3
Biennial Follow-Up Review
Data Collection & Maintenance Review
Member Enrollment & Re-Enrollment Review
Member Retirement Application & Eligibility Review
Disability Hearing & Contested Cases Process Review

Benefit Estimates & Final Benefit Calculation Processing Review
Unclaimed Member Benefits & Accounts Review
Member Counseling & Communication Review
IT Governance Content Development
Virtual Chief Information Security Officer (vCISO)
Identity Access & Management Risk Assessment
Identity Access & Management Risk Assessment
IT Security Rapid Assessment™ & Security Review
Cloud Risk and Security Assessment - Phase 1
Cloud Risk and Security Assessment - Phase 2
vCISO Initiative - Roadmap Implementation
Disaster Recovery Gap Assessment
IT General Controls (ITGC) Review - Financial and Pension Systems
Backup, Data Recovery, and Data Retention Assessment
IT Architecture Analysis
Cybersecurity, Vulnerability and Patch Management Assessment

Proposed Two-Year Internal Audit Plan

Proposed Audit Plan - 2025

The following represents the detailed Internal Audit Plan which covers the period from January 1, 2025 through December 31, 2025.

Internal Audit Plan – January 1, 2025 through December 31, 2025

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
2024 CARRYOVER PROJECTS				
<p>Investment Manager Selection and Evaluation Review</p> <p>Project objectives include:</p> <ul style="list-style-type: none"> • Evaluate the Investment Office’s compliance with the requirements and internal controls set forth in the ERS’ Investment Manager Selection Process Framework; which is comprised of stages to identify, evaluate, recommend, and approve prospective investment managers. • Assess whether the ERS’ Investment Manager Selection Process Framework aligns with leading practices recommended by professional investment organizations and/or performed by peer pension systems in order to identify opportunities to enhance the current framework. • Provide recommendations and leading practices for improvements to enhance effectiveness and efficiency, where applicable. <p>PRIMARY FOCUS: Operational/Financial</p>	<p>Investment Office <i>Investment Management Evaluation & Selection</i></p>	<p>Authority/Limit Risk Alignment Risk Efficiency Risk Performance Gap Risk Service Failure Risk</p>	<p>Q1</p>	<p>150</p>
<p>Contracting & Procurement Review</p> <p>Assess and review the processes and controls related to contracting and procurement. This includes the review of policies and procedures, management and prioritization of procurement requests, internal controls on the preparation and finalization of procurements and associated contracting, and maintenance and retention of documentation. As applicable, evaluate the ERS' compliance with applicable HAR, HRS and Administrative Directives.</p> <p>PRIMARY FOCUS: Operational/Compliance</p>	<p>Administration <i>Contracting & Procurement</i></p>	<p>Business Interruption Risk Compliance Risk Cycle Time Risk Efficiency Risk Performance Gap Risk Service Failure Risk</p>	<p>Q1</p>	<p>375</p>

TOTAL PROPOSED CARRYOVER HOURS: 01/25 - 12/25 525

Proposed Audit Plan - 2025

Internal Audit Plan – January 1, 2025 through December 31, 2025

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ASSURANCE				
<p>Benefit Claims & Refund and Retiree Overpayments Processing Review</p> <p>Evaluate processes and procedures around disbursements of benefit payments with specific focus on retiree overpayments and benefit claims and refunds. Review and assess whether benefit claims, refunds, and overpayments are processed accurately, uniformly, and timely in compliance with HRS, HAR, IRS, and Administrative Directives. Assess the internal controls over the refunding process and procedures to identify deficiencies that lead to overpayment of benefit claims.</p> <p>PRIMARY FOCUS: Operational/Financial</p>	<p>Accounting</p> <p><i>Benefit Claims & Refund Audit</i></p> <p><i>Processing of Retiree Overpayments</i></p> <p><i>Disbursements of Benefit Payments</i></p>	<p>Compliance Risk</p> <p>Customer Satisfaction Risk</p> <p>Cycle Time Risk</p> <p>Efficiency Risk</p> <p>Performance Gap Risk</p> <p>Service Failure Risk</p>	Q2	400
<p>Member/Retiree Record Processing, Retention, and Storage</p> <p>Assess the design of processes and internal controls over the initial intake and processing, retention, and storage of ERS files, including member enrollment and retirement records, in order to efficiently and effectively retrieve records, as needed. Evaluate whether processes align with HRS, HAR, departmental records retention schedules, and guidance provided by the State of Hawaii Records Management Branch.</p> <p>PRIMARY FOCUS: Operational/Compliance</p>	<p>Staff Support Services</p> <p><i>Member/Retiree Record Retention and Storage Data</i></p>	<p>Availability Risk</p> <p>Compliance Risk</p> <p>Access Risk</p> <p>Regulatory Risk</p> <p>Efficiency Risk</p>	Q4	350

Proposed Audit Plan - 2025

Internal Audit Plan – January 1, 2025 through December 31, 2025

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ASSURANCE				
<p>Business Continuity Plan – Tabletop Exercise</p> <p>Conduct tabletop exercise focusing on the downtime procedures and workaround activities for Support Services, Accounting, Retirement Benefits Branch and the Investment Office in the event of a significant disruption to multiple critical systems and applications. The exercise emphasizes the enhancement of operational continuity resilience for ERS through discussion of the execution of their documented continuity actions. The exercise will aim to identify opportunities for improvements based on lessons learned from real life disruption events not only in Hawaii but also in the continental U.S. and globally.</p> <p><i>PRIMARY FOCUS: Operational</i></p>	<p>Information Systems <i>Business Continuity & Disaster Recovery Planning</i> <i>Data Retention & Backup</i></p> <p>Administration <i>Crisis Management and Communication</i></p>	<p>Availability Risk Customer Satisfaction Risk Infrastructure Risk Service Failure Risk Catastrophic Loss Risk Communications Risk</p>	Q3	250
TOTAL PROPOSED ASSURANCE HOURS: 01/25 - 12/25				1,000

Proposed Audit Plan - 2025

Internal Audit Plan – January 1, 2025 through December 31, 2025

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ADVISORY				
<p>vCISO Initiative - Roadmap Implementation</p> <p>Continue to provide a C-level resource to implement the Cybersecurity Strategy and Roadmap as defined and developed as part of the Phase 1 project. Implementation activities will focus on priorities that align with the organization's business and strategic plans, while addressing the risk posture of the organization. Activities to include the following: define timetable and priorities for remediation of previous audit findings, security steering committee initiation, vendor risk assessments, IT and security policy development, cybersecurity awareness trainings, and establishment of a vulnerability management program. The duration of the project is expected to last for approximately six months.</p> <p>PRIMARY FOCUS: Operational/Information Technology</p>	Various (Org-wide)	Various Risks	Q1	750
<p>ERM Capability Roadmap and Training</p> <p>Working with ERS' Management Team, understand the current state of risk management activities in the organization, and deliver training to key stakeholders to increase the education and awareness of the enterprise risk management (ERM) function. Develop an initial roadmap outlining best practices to develop the ERM function.</p> <p>PRIMARY FOCUS: Operational/Compliance</p>	Various (Org-wide)	Various Risks	Q2	250

Proposed Audit Plan - 2025

Internal Audit Plan – January 1, 2025 through December 31, 2025

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ADVISORY				
<p>Continuous Monitoring Tool Development - Part 2</p> <p>Continue to build upon the ideas and opportunities identified in Part 1 to create and develop a continuous monitoring tool or platform to assist in tracking and monitoring employer compliance with ERS reporting requirements. A tool will be developed to monitor timely submission of payroll reports and proper submission of overpayment adjustments. IA will meet and collaborate with the Employer Reporting Team and the Compliance Office to develop a tool that aligns with their monitoring needs. Training will be provided to ensure that branches are able to properly own and use the tool for future use.</p> <p>PRIMARY FOCUS: Operational/Information Technology</p>	Various (Org-wide)	Various Risks	Q3	550
<p>IA Recommendation & Implementation Assistance</p> <p>Assist ERS in implementing prior year internal audit report recommendations that have not been cleared due to lack of sufficient resources to address them in a timely manner. KMH will be collaborating and prioritizing with ERS' various branches to implement high, medium, and low risk recommendations.</p> <p>PRIMARY FOCUS: Operational/Compliance/Financial</p>	Various (Org Wide)	Various Risks	Ongoing	100
TOTAL PROPOSED ADVISORY HOURS: 01/25 - 12/25				1,650

Proposed Audit Plan - 2025

Internal Audit Plan – January 1, 2025 through December 31, 2025

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
OTHER				
Function Administration - January 1, 2025 - December 31, 2025				
Internal Audit Plan Update for Year 4			Q4	100
Compliance Office Collaboration and Assistance			Throughout	150
Reporting, Communication and Other Administration			Throughout	350
TOTAL OTHER HOURS: 01/25 - 12/25				600
TOTAL PROPOSED HOURS: 01/25 - 12/25				3,775

Proposed Audit Plan - 2026

The following represents the detailed Internal Audit Plan which covers the period from January 1, 2026 through December 31, 2026.

Internal Audit Plan – January 1, 2026 through December 31, 2026

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ASSURANCE				
<p>Biennial Follow-Up Review</p> <p>Assess the progress that responsible managers made in implementing prior finding recommendations for previously completed reviews between 2023 and 2025 as well as finding recommendations remediated for reviews completed prior to 2023. This includes recommendations from reviews completed on the following ERS branches/areas: Administration, Program Support, Retirement Benefits, Accounting, Staff Support Services, and Investment Office. Assessment includes evaluating the design and operation of newly implemented internal controls and processes.</p> <p>PRIMARY FOCUS: Operational/Compliance/Financial</p>	Various (Org-wide)	<p>Cycle Time Risk</p> <p>Efficiency Risk</p> <p>Performance Gap Risk</p> <p>Service Failure Risk</p>	Q1	300
<p>Investment Management, Monitoring & Performance Evaluation</p> <p>Assess the design of processes and internal controls over the management and monitoring of ERS's investment managers, Investment Office's compliance with performance evaluation procedures, and where appropriate, review investment managers compliance with their respective contract restrictions and requirements.</p> <p>PRIMARY FOCUS: Operational/Financial</p>	<p>Investment Office</p> <p>Investment Management,</p> <p>Monitoring & Performance</p> <p>Evaluation</p>	<p>Organization Structure Risk</p> <p>Authority/Limit Risk</p> <p>Alignment Risk</p> <p>Efficiency Risk</p>	Q2	450

Proposed Audit Plan - 2026

Internal Audit Plan – January 1, 2026 through December 31, 2026

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ASSURANCE				
<p>Investment Accounting</p> <p>Assess the design of processes and internal controls over the accounting of investments to ensure that ERS maintains conformity with applicable Governmental Accounting Standards Board (GASB) standards and guidance, activities comply with ERS policies and procedures, investment balances are accurate and properly valued, and accounting records reconciles to the custodial bank's book of record.</p> <p>PRIMARY FOCUS: Operational/Compliance/Financial</p>	<p>Accounting</p> <p><i>Investment Accounting & Compliance Reporting</i></p>	<p>Financial Reporting</p> <p>Evaluation Risk</p> <p>Compliance Risk</p> <p>Integrity Risk</p> <p>Availability Risk</p>	Q3	450
<p>V3locity Business Readiness Assessment</p> <p>The V3locity Business Readiness Assessment will assist ERS in identifying and understanding organizational risk with their cloud based pension administration system implementation. The assessment will evaluate the organization's approach to business process decisions and requirements, and management plans over testing, data conversion, go-live deployment and criteria, implementation and failover, organizational change management and training, and post-implementation production support. The objective is to identify leading practice recommendations to be considered and incorporated as part of the eventual go-live implementation of V3locity.</p> <p>PRIMARY FOCUS: Operational/Information Technology</p>	<p>Information Systems</p> <p><i>IT Change Management</i></p> <p><i>Information Security</i></p> <p><i>Event, Incident & Problem Management</i></p> <p><i>IT Vendor/Third Party Management</i></p>	<p>Availability Risk</p> <p>Communications Risk</p> <p>Infrastructure Risk</p> <p>Security Risk</p> <p>Service Failure Risk</p> <p>Technological Innovation Risk</p>	Q3	500
TOTAL PROPOSED ASSURANCE HOURS: 01/26 - 12/26				1,700

Proposed Audit Plan - 2026

Internal Audit Plan – January 1, 2026 through December 31, 2026

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
ADVISORY				
<p>Continuous Monitoring Tool Development - Part 3</p> <p>Continue to create and develop a continuous monitoring tool or platform to assist in tracking and monitoring employer compliance with ERS' payroll and personnel reporting requirements. IA will meet and collaborate with applicable branches to develop a tool that aligns with their monitoring needs. Training will be provided to ensure that branches are able to properly own and use the tool for future use.</p> <p>PRIMARY FOCUS: Operational/Information Technology</p>	Various (Org Wide)	Various Risks	Q1	450
<p>IA Recommendation & Implementation Assistance</p> <p>Assist ERS in implementing prior year internal audit report recommendations that have not been cleared due to lack of sufficient resources to address them in a timely manner. KMH will be collaborating and prioritizing with ERS' various branches to implement high, medium, and low risk recommendations.</p> <p>PRIMARY FOCUS: Operational/Compliance/Financial</p>	Various (Org Wide)	Various Risks	Ongoing	100
TOTAL PROPOSED ADVISORY HOURS: 01/26 - 12/26				550

Proposed Audit Plan - 2026

Internal Audit Plan – January 1, 2026 through December 31, 2026

Project	Auditable Area(s)	Quadrant I Risk(s)	Timing	Est. Hrs.
OTHER				
Function Administration - January 1, 2026 - December 31, 2026				
Risk Assessment Re-Evaluation & Two-Year Audit Plan			Q4	250
Compliance Office Collaboration and Assistance			Throughout	150
Reporting, Communication and Other Administration			Throughout	350
TOTAL OTHER HOURS: 01/26 - 12/26				750
TOTAL PROPOSED HOURS: 01/26 -12/26				3,000

Proposed Two-Year Internal Audit Plan Schedule

2025 Proposed Internal Audit Plan Schedule

The chart below depicts the proposed timing of the projects included in the Internal Audit Plan. The diamonds and bars are meant to portray the approximate project duration, including the estimated start and end dates of each project.

Internal Audit Plan Period: January 1, 2025 through December 31, 2025														
PROJECT	Q1 2025			Q2 2025			Q3 2025			Q4 2025			Hours	
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Budget	
2024 Carryover Projects														
Investment Manager Selection & Evaluation Review	[In Process]												150	
Contracting & Procurement Review	[In Process]			[In Process]									375	
Assurance														
Benefit Claims & Refund and Retiree Overpayments Processing Review					◆								400	
Member/Retiree Record Processing, Retention, and Storage										◆			350	
Business Continuity Plan – Tabletop Exercise							◆						250	
Advisory & Other														
vCISO Initiative - Roadmap Implementation	◆	[Consulting & Other Projects]						◆						750
ERM Capability Roadmap and Training				◆									250	
Continuous Monitoring Tool Development - Part 2								◆					550	
IA Recommendation & Implementation Assistance	◆	[Consulting & Other Projects]											◆	100
Internal Audit Plan Update for Year 4											◆	◆	100	
Compliance Office Collaboration and Assistance	◆	[Meetings, Board Support, Other]											◆	150
Reporting, Communication and Other Administration	◆	[Meetings, Board Support, Other]											◆	350
												Total Hours	3,775	



The timing and execution of the projects included in the proposed Audit Plan may change. Significant changes to the Audit Plan will be communicated to the Administrative & Audit Committee on a periodic basis.

2026 Proposed Internal Audit Plan Schedule

Internal Audit Plan Period: January 1, 2026 through December 31, 2026													
PROJECT	Q1 2026			Q2 2026			Q3 2026			Q4 2026			Hours
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Budget
Assurance													
Biennial Follow-Up Review	◆												300
Investment Management, Monitoring & Performance Evaluation				◆									450
Investment Accounting									◆				450
V3locity Business Readiness Assessment							◆						500
Advisory & Other													
Continuous Monitoring Tool Development - Part 3		◆											450
IA Recommendation & Implementation Assistance	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	100
Risk Assessment Re-Evaluation & Two-Year Audit Plan										◆	◆	◆	250
Compliance Office Collaboration and Assistance	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	150
Reporting, Communication and Other Administration	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	350
												Total Hours	3,000

◆ Project Start Date
 ◆—◆ Consulting & Other Projects
 ◆- - ◆ Meetings, Board Support, Other

The timing and execution of the projects included in the proposed Audit Plan may change. Significant changes to the Audit Plan will be communicated to the Administrative & Audit Committee on a periodic basis.

Appendices

- Appendix A – Interview List
- Appendix B – Relevant Risk Definitions: Quadrant I
- Appendix C – Relevant Risk Definitions: Other Quadrants

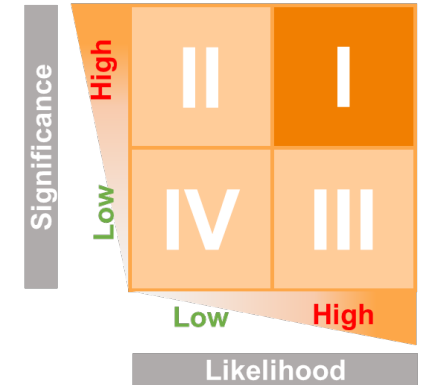
Appendix A - Interview List

IA conducted interviews with various members of the management team, members of the Board, and other associated parties. The objectives of these interviews were to identify and discuss relevant risks, confirm the auditable areas, and obtain a high-level understanding of the controls and processes in place to mitigate relevant risks. The following is a list of the individuals interviewed:

- Thom Williams, Executive Director
- Kristen Varela, Chief Investment Officer
- Kona Mann, Chief Compliance Officer
- Lori Kobayashi, Retirement Benefits Branch Manager
- Larry Wolfe, Accounting Manager
- Keith Miyamoto, Information Technology Manager
- James Greubel, Program Specialist
- Drew Tomimoto, Staff Support Services Supervisor
- Bennett Yap, Trustee and Board Chair
- Catherine Chan, Trustee and Administrative & Audit Committee Chair
- Vincent Barfield, Trustee and Administrative & Audit Committee Vice Chair
- Genevieve Ley, Trustee
- Lance Mizumoto, Trustee
- Luis Salaveria, Trustee
- Bennett Yap, Trustee
- Ralph Kanetoku, Robyn Kawamura, and YeeYan Lim, External Auditor (KKDLY)

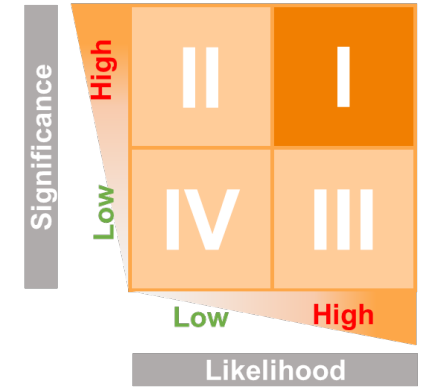
Appendix B – Relevant Risk Definitions: Quadrant I

Risk	Definition
Access Risk	Access risk includes the risk that access to information (data or programs) or systems will be inappropriately granted or refused. It encompasses the risks of improper segregation of duties, risks associated with the integrity of data and databases and risks associated with information confidentiality.
Accounting Information Risk	Financial accounting information used to manage business processes is not properly integrated with nonfinancial information focused on customer satisfaction, measuring quality, reducing cycle time and increasing efficiency. The result is a myopic, short-term fixation on manipulating the outputs of business processes to achieve financial targets, rather than fulfilling customer expectations by controlling and improving processes.
Alignment Risk	The objectives and performance measures of the organization's business processes are not aligned with its overall business objectives and strategies. The objectives and measures do not focus people on the right things and lead to conflicting, uncoordinated activities.
Business Interruption Risk	The organization's capability to continue critical operations and processes may be highly dependent on availability of certain information technologies, skilled labor and other resources.
Capital Availability Risk	The organization does not have efficient access to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.



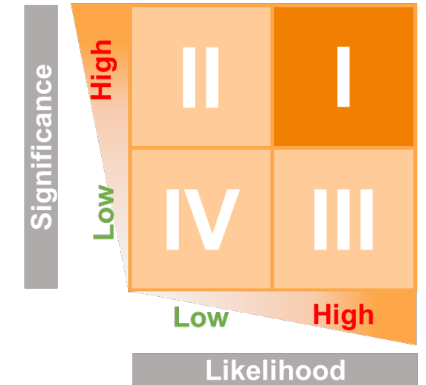
Appendix B – Relevant Risk Definitions: Quadrant I (continued)

Risk	Definition
Communications Risk	Communication channels (top-down and bottom-up or cross-functional) within the organization are ineffective and result in messages that are inconsistent with authorized responsibilities or established measures.
Compliance Risk	As a result of a flaw in design or operation or due to human error, oversight or indifference, the organization's processes do not meet customer requirements the first time or do not comply with prescribed procedures and policies. Compliance risk can also result in failure to conform with laws and regulations at the international, federal, state and local level that apply to a business process.
Contract Commitment Risk	The organization does not have information that effectively tracks contractual commitments outstanding at a point in time, so that the financial implications of decisions to enter into incremental commitments can be appropriately considered by decision makers.
Credit Risk	The exposure to actual loss or opportunity cost as a result of default (or other failure to perform) by an economic or legal entity (the debtor) with which the organization does business.
Customer Satisfaction Risk	The organization's processes do not consistently meet or exceed customer expectations due to a lack of focus on the customer.
Cycle Time Risk	Elapsed time between the start and completion of a business process (or activity within a process) is too long because of redundant, unnecessary and irrelevant steps.



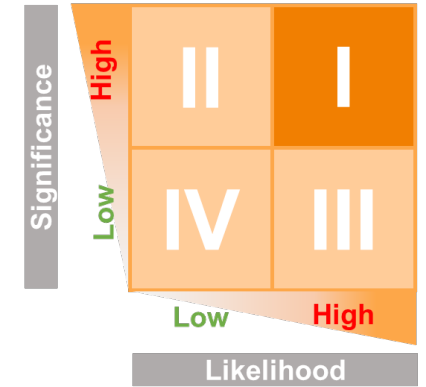
Appendix B – Relevant Risk Definitions: Quadrant I (continued)

Risk	Definition
Efficiency Risk	The process is inefficient in satisfying valid customer requirements resulting in higher costs.
Financial Markets Risk	Financial markets risk is defined as exposure to changes in the earnings capacity or economic value of the organization as a result of changes in financial market variables (e.g., currency, interest rates). These changes affect income, expense or balance sheet values.
Human Resources Risk	The personnel responsible for managing and controlling the organization or a business process do not possess the requisite knowledge, skills and experience needed to ensure that critical business objectives are achieved and significant business risks are reduced to an acceptable level.
Infrastructure Risk	The risk that the organization does not have an effective information technology infrastructure (e.g., hardware, networks, software, people and processes) to effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion.
Knowledge Capital Risk	Processes for capturing and institutionalizing learning across the organization are either nonexistent or ineffective, resulting in slow response time, high costs, repeated mistakes, slow competence development, constraints on growth and unmotivated employees.
Leadership Risk	The risk that the people responsible for the important business processes do not or can not provide the leadership, vision, and support necessary to help employees be effective and successful in their jobs.



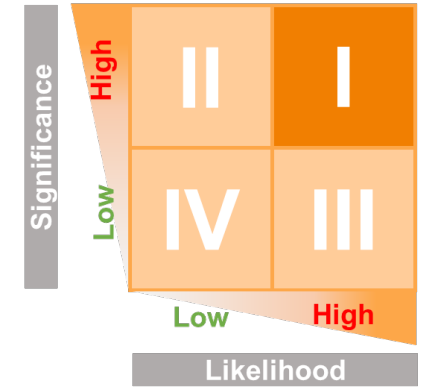
Appendix B – Relevant Risk Definitions: Quadrant I (continued)

Risk	Definition
Organization Structure Risk	The organization's structure does not support change or the organization's business strategies.
Organizational Culture Risk	The organization's culture does not encourage managers to realistically portray the potential outcomes of transactions, deals, investments and projects and understand and portray the full picture for decision makers. The organization experiences dysfunctional behavior because managers are either risk averse or incented to take risks beyond the organization's risk appetite.
Performance Gap Risk	A business process does not perform at a "best-of-class" level because the practices designed into the process are inferior.
Privacy Risk	Privacy encompasses the rights and obligations of individuals and the organization with respect to the collection, use, retention, disclosure, and disposal of personal information.
Regulatory/Legislative Risk	Changes in regulations or laws and actions by national or local regulators/legislators can result in increased competitive pressures and required changes in business processes, which significantly affect the organization's ability to efficiently conduct business.
Resource Allocation Risk	The organization's resource allocation process does not generate and sustain effective and efficient operations or maximize returns for stakeholders.



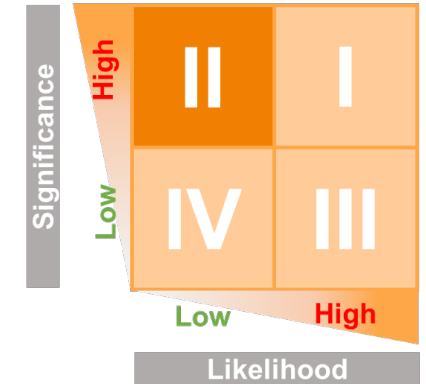
Appendix B – Relevant Risk Definitions: Quadrant I (continued)

Risk	Definition
Security Risk	The risk that a possible threat will use a vulnerability in the system of the organization to cause disruption to the organizational assets, operations and/or objectives.
Service Failure Risk	The organization's operations create risk of customers receiving faulty or nonperforming services.
Succession Planning Risk	Leadership talent within the organization is not sufficiently developed to provide for orderly succession in the future.
Technological Innovation Risk	The organization is not leveraging advancements in technology in its business model to attain superior quality, cost and/or time performance in its services and processes.



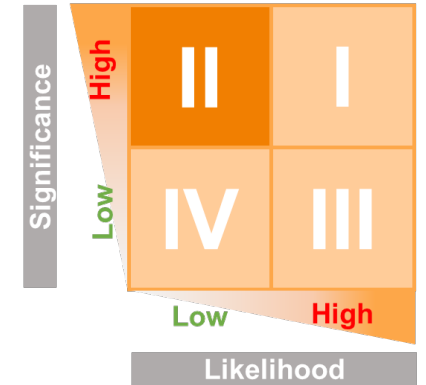
Appendix C – Relevant Risk Definitions: Quadrant II

Risk	Definition
Authority/Limit Risk	The risk that people either make decisions or take actions that are not within their explicit responsibility or control or fail to take responsibility for those things for which they are accountable. Failure to establish or enforce limits on personnel actions may cause employees to commit unauthorized, illegal or unethical acts or assume unauthorized or unacceptable business risks.
Availability Risk	The risk that information will not be available when needed. This includes risks such as loss of communications (e.g., cut cables, telephone system outage, satellite loss), loss of basic processing capability (e.g., fire, flood, electrical outage) and operational difficulties (e.g., data server breakdown, operator errors).
Budget and Planning Risk	Budgets and business plans are not 1) realistic, 2) based on appropriate assumptions, cost drivers, and performance measures, 3) accepted by key managers, or 4) used as a monitoring tool.
Catastrophic Loss Risk	The inability to sustain operations, provide services, or recover operating costs as a result of a major disaster.
Customer Wants Risk	The organization is not aware that customer needs and wants change. Such needs and wants may apply to desired service quality, willingness to pay and/or speed of execution.
Ethical Behavior Risk	The organization, through its actions or inaction, demonstrates that it is not committed to ethical and responsible business behavior.



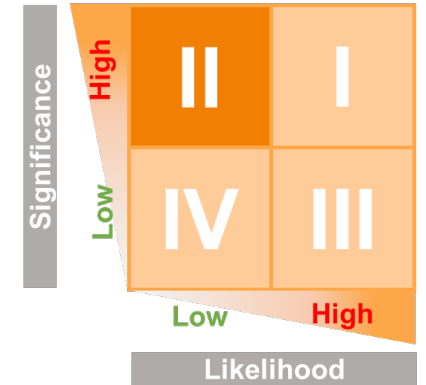
Appendix C – Relevant Risk Definitions: Quadrant II (continued)

Risk	Definition
Image and Branding Risk	The risk that the organization may lose its key employees or its ability to maintain public confidence, due to perceptions that it does not deal fairly with customers, suppliers and stakeholders, or know how to manage its business.
Integrity Risk	This risk encompasses all of the risks associated with the authorization, completeness, and accuracy of transactions as they are entered into, processed by, summarized by and reported on by the various application systems deployed by the organization.
Investment Valuation/Evaluation Risk	Management does not have sufficient financial information to make informed short-term and long-term investment decisions and link the risks accepted to the capital at risk. Management and key decision-makers are unable to reliably measure the value of the organization's investment portfolio in a strategic context.
Legal Risk	The risk that the organization's transactions, contractual agreements and specific strategies and activities are not enforceable under applicable law.
Liquidity Risk	The exposure to loss as a result of the inability to meet cash flow obligations in a timely and cost-effective manner. Liquidity risk often arises as a result of an investment portfolio with a cash flow and/or maturity profile, which differs from the underlying cash flows dictated by the organization's operating requirements and obligations.



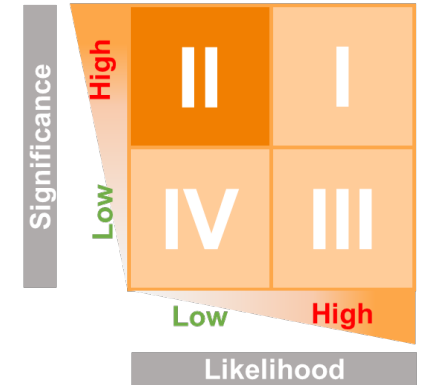
Appendix C – Relevant Risk Definitions: Quadrant II (continued)

Risk	Definition
Measurement (Strategy) Risk	Occurs when overall organizational performance measures focus primarily on near-term financial results or are not consistent with and do not support business strategies.
Outsourcing Risk	Outside service providers do not act within their defined limits of authority and do not perform in a manner consistent with the values, strategies and objectives of the organization.
Portfolio Risk	The risk that the organization will not maximize business and financial performance by effectively balancing its portfolio in a strategic context.
Price Risk	The exposure of earnings or net worth to changes in market factors (e.g., interest rates, currency rates, commodity, financial instrument), which affect income, expense or balance sheet values.
Regulatory Reporting Risk	Reports of operating and financial information required by regulatory agencies are incomplete, inaccurate, or untimely, exposing the organization to fines, penalties and sanctions.
Sovereign/Political Risk	The risk of adverse consequences through political actions in a country in which the organization has made significant investments, is dependent on a significant volume of business or has entered into an agreement with a counter party subject to the laws of that country.
Stakeholder Relations Risk	A decline in stakeholder confidence may impair the organization's ability to efficiently raise capital. The organization will not have the same efficient access to the capital it needs to fuel its growth, execute its strategies, and generate future financial returns.



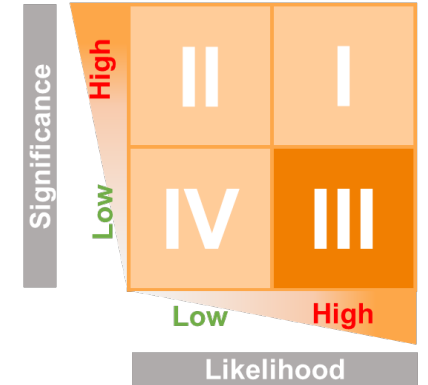
Appendix C – Relevant Risk Definitions: Quadrant II (continued)

Risk	Definition
Taxation Risk	Significant transactions of the organization have adverse tax consequences that could have been avoided had they been structured differently. Failure to comply with all tax regulations (e.g., payment and filing requirements) creates risks.



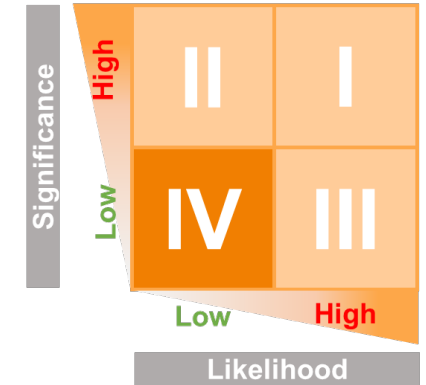
Appendix C – Relevant Risk Definitions: Quadrant III

Risk	Definition
Board Effectiveness Risk	The Board does not constructively engage management and provide anticipatory, proactive and interactive oversight of the organization's activities and affairs, with integrity, vision, common sense and unquestioned independence.
Change Readiness Risk	The people within the organization are unable to implement process and service improvements quickly enough to keep pace with changes in the marketplace or changes required by legislation.
Financial Reporting Evaluation Risk	Financial reports issued to existing and prospective investors and lenders include material misstatements or omit material facts, making them misleading.
Internal Control Evaluation Risk	Failure to accumulate sufficient relevant and reliable information to assess the design and operating effectiveness of internal control over financial reporting, resulting in inaccurate assertions by management in the internal control report.
Sensitivity Risk	Sensitivity risk results when management commits the organization's resources and expected cash flows from future operations to such an extent that it reduces the organization's tolerance for (or ability to withstand) changes in environmental forces that are totally beyond its control.



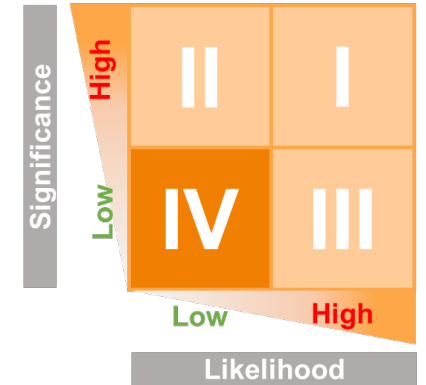
Appendix C – Relevant Risk Definitions: Quadrant IV

Risk	Definition
Business Model Risk	The organization has an obsolete business model and does not recognize it and/or lacks the information needed to make an up-to-date assessment of its current model and build a compelling business case for modifying that model on a timely basis.
Employee Fraud and Third Party Fraud Risk	Fraudulent activities perpetrated by employees, customers, suppliers, agents, brokers or third-party administrators against the organization for personal gain expose the organization to financial loss.
Environmental Scan Risk	The failure to monitor and stay in touch with a rapidly changing environment resulting in obsolete business strategies.
Health and Safety Risk	These risks expose the organization to potentially significant workers' compensation liabilities, financial loss, and negative publicity. The organization and its managers could find themselves liable for failure to provide a safe working environment for their employees.
Illegal Acts Risk	Managers and employees individually or in collusion commit illegal acts, placing the organization, its trustees, and officers at risk to the consequences of their actions.
Management Fraud Risk	Management issues misleading financial statements with intent to deceive the public and the external auditor or engages in bribes, kickbacks, influence payments and other schemes for the benefit of the organization.

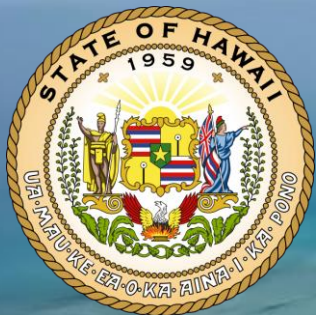


Appendix C – Relevant Risk Definitions: Quadrant IV (continued)

Risk	Definition
Measurement (Operations) Risk	Process performance measures do not provide a reliable portrayal of operating performance and do not accurately reflect reality. The measures do not provide relevant information for decision making because they are not informative, understandable, believable, actionable, or indicators of change.
Performance Incentives Risk	Unrealistic, subjective or unclear performance measures may cause managers and employees to act in a manner that is inconsistent with the organization's business objectives, strategies, ethical standards and prudent business practice.
Planning Risk	The organization's business strategies are not driven by creative and intuitive input or based on current assumptions about the external environment resulting in strategies that are out-of-date and unfocused.
Unauthorized Use Risk	The organization's employees (or others) use its physical and financial assets for unauthorized or unethical purposes.



Employees' Retirement System of the State of Hawaii

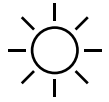


Employees' Retirement System
of the State of Hawaii

Compliance Quarterly Update
Kona Mann
February 2025

Executive Summary:

This is the CCO's quarterly update. Report is being presented for Committee's awareness & discussion.



Key Highlights

- Compliance Activities Completed: GRC Platform RFP issued and bids are being reviewed.
- Compliance Opportunities:
 - vCISO, Data & Analytics (D&A), Risk Management, and IT - Develop D&A and Risk Management Strategy, support vCISO Roadmap activities, support IT security and strategic planning, and tech and vendor acquisition;
 - Governance Functions - Velocity Migration Project Management, Automation Initiatives, Business Continuity Planning and (3) Lines of Defense (independent);
 - Employer Reporting - Audit Plan, Audit Support (KMH, Accounting, RBB);
 - Compliance - Record Retention & Disposal, RM Framework and Reporting, Code of Ethics & Business Conduct, and Policy Workshops with Branches & KMH/RSM;.



Next Steps

- Compliance will continue to support branch operational activities and align compliance and risk program implementation activities.
- Work will continue to support ERS' goal of responsible governance by assisting branches with developing and implementing priorities to include establishing policies and goals.



ERS Compliance Program

- **STRATEGY:** Compliance is central to ERS' strategic planning;
 - Using tools, strategies, data and all stakeholders to make informed decisions
 - Establish consistency in operational strategic planning supported by data, informed by risk and compliance, aligned to organizational goals and objectives.
 - Utilize data and analytics, risk management, internal audit, and compliance activities to support continuous improvement.
- **RISK MANAGEMENT:** Risks are identified, owned, prioritized and managed;
 - Branches Are Aware & Own Risks
 - Process development, mapping, ownership and management.
 - Risk-enabled processes, dashboard reporting, clear decision-making and calendared activities.
- **CULTURE:** Leaders at all levels across the organization build and sustain a culture of integrity & risk governance and management;
 - Continue building risk aware culture
 - Continuing supporting process ownership and drive policy and procedure development.
 - Provide education, training and support.
- **ACCOUNTABILITY:** ERS and its various business functions take action and holds itself accountable to effective risk management and open and upward communication, sharing of knowledge and best practices, continuous process improvement and a strong commitment to ethical and responsible business behavior.
 - Discipline & Enforcement.



MINUTES OF THE MEETING OF THE
ADMINISTRATIVE AND AUDIT COMMITTEE OF THE BOARD OF TRUSTEES OF THE
EMPLOYEES' RETIREMENT SYSTEM OF THE STATE OF HAWAII

OCTOBER 23, 2024

CITY FINANCIAL TOWER
201 MERCHANT STREET, SUITE 1200
HONOLULU, HAWAII 96813

Trustees present: Dr. Catherine Chan, Chair*
(City Financial Tower Mr. Vincent Barfield, Vice Chair*
by teleconference) Dr. Genevieve Ley*

Trustee absent: Mr. Luis Salaveria

Staff present: Mr. Thomas Williams, Executive Director*
(City Financial Tower Mr. Kona Mann, Chief Compliance Officer*
by teleconference) Mr. James Greubel, Program Specialist*
Ms. Kristin Varela, Chief Investment Officer*
Ms. Sandra Straub, Information Services Systems Supervisor*
Ms. Dale Kehau Kanae, Recording Secretary/Administrative Assistant*
Ms. Lori Kim, Administrative Assistant
Ms. Andrea Gasper, Administrative Assistant*

Attorneys present: Ms. Jenny Nakamoto, Deputy Attorney General*
(by teleconference) Ms. Lori Tanigawa, Deputy Attorney General*
Ms. Elmira Tsang, Deputy Attorney General*
Ms. Diane Wong, Deputy Attorney General*

Guests present: Mr. Peter Hanashiro, KMH LLP
(by teleconference) Mr. Tyson Suehiro, KMH LLP
Mr. Dave Collins, RSM US LLP
Mr. Alfred Ko, RSM US LLP

*Attended Executive Session

QUORUM/CALL TO ORDER

A quorum being present (Chair Chan, Vice Chair Barfield, and Trustee Ley), Chair Chan called the meeting of the Administrative and Audit Committee (Committee) of the Board of Trustees (Board) of the Employees' Retirement System of the State of Hawaii (ERS) to order at 2:00 p.m. and identified the Trustees present and had them confirm that they are the only ones present at their remote location and that no one else was able to listen in on their teleconference while attending the meeting.

On a motion made by Trustee Ley, seconded by Vice Chair Barfield, and unanimously carried, the Committee voted to hold a meeting allowing Trustees and members of the public to participate by interactive conference technology, pursuant to the HRS §92-3.7, with at least one meeting location open to the public that has audiovisual connection.

PUBLIC COMMENT

Chair Chan called for public comment. There was no public present by teleconference or in person, therefore, no public comment. There was also no written public testimony received for this Committee meeting.

INTERNAL AUDIT UPDATE
REPORT BY KMH LLP ON
THE CURRENT STATUS OF
ACTIVITIES COMPLETED
DURING Q3, 2024, AND AN
UPDATE ON THE
COMPLETION STATUS OF
MANAGEMENT ACTION
PLANS FOR PAST INTERNAL
AUDIT OBSERVATIONS AND
RECOMMENDATIONS

KMH LLP’s Peter Hanashiro and Tyson Suehiro attended the meeting in person and presented oral and written reports to the Committee of KMH LLP’s Internal Audit Update Report and Follow-Up Review Report on the Current Status of Previously “Cleared” Internal Audit Observations and Recommendations and discussed in part, and summary:

INTERNAL AUDIT UPDATE REPORT
EXECUTIVE SUMMARY

Administrative and Other Matters
Status on Current Projects

- Follow-Up Review
- Virtual Chief Information Security Officer (vCISO)
- Continuous Monitoring Tool Development – Part 2
- Investment Manger Selection and Evaluation Review
- Risk Assessment Re-Evaluation and Audit Plan

SUMMARY RESULTS OF REPORTS COMPLETED

2024 Follow-Up Review

- Background and Project Objectives
- Summary of Results

2024 INTERNAL AUDIT PLAN RESULTS SUMMARY

MANAGEMENT ACTION DASHBOARD

MANAGEMENT ACTION PLANS – COMPLETION STATUS

CUMULATIVE OBSERVATION ANALYSIS

ISSUED REPORTS FINDING STATUS

There was no action required of the Committee for this agenda item.

FOLLOW-UP REVIEW
REPORT BY KMH LLP ON
THE CURRENT STATUS OF
PREVIOUSLY “CLEARED”
INTERNAL AUDIT
OBSERVATIONS AND
RECOMMENDATIONS

FOLLOW-UP REVIEW
EXECUTIVE SUMMARY

Background
Project Objectives
Overall Assessment and Conclusion

FOLLOW-UP REVIEW PROCESS

Follow-Up Review Process – Overview
Reports Selected and Number of Findings

FINDINGS REVIEWED AND SUMMARY OF RESULTS

Summary of Follow-Up Review Results

INVESTMENT AND RISK MONITORING AND REPORTING
REVIEW

FINANCIAL REPORTING PROCESS REVIEW

INVESTMENT CONSULTANT SELECTION AND EVALUATION
REVIEW

COMMUNICATIONS AND COMMUNITY RELATIONS REVIEW

HR – PERSONNEL DEVELOPMENT & RETENTION REVIEW

BENEFIT ESTIMATES & FINAL BENEFIT CALCULATION

PROCESSING REVIEW

The Committee requested KMH LLP include the finding ratings in the table of Summary of Follow-Up Review Results, reference pg. 10 of the report.

FOLLOW-UP REVIEW
REPORT BY KMH LLP ON
THE CURRENT STATUS OF
PREVIOUSLY “CLEARED”
INTERNAL AUDIT
OBSERVATIONS AND
RECOMMENDATIONS
(CONT’D)

On a motion made by Vice Chair Barfield, seconded by Trustee Ley, and unanimously carried, the Committee accepted KMH LLP’s Follow-Up Review Report on the Current Status of Previously “Cleared” Internal Audit Observations and Recommendations and will be presenting it to the Board for their approval at the next Board meeting of November 12, 2024.

COMPLIANCE SUPPORT
STAFF REPORT ON GENERAL
DUTIES AND CURRENT AND
FUTURE PROJECTS

Chief Compliance Officer (CCO) Kona Mann requested that his Compliance Support Staff Report on General Duties and Current and Future Projects be deferred, however, noted that some of the current projects being worked on would be discussed in Executive Session.

REPORT BY PROGRAM
SPECIALIST ON THE
IMPLEMENTATION OF THE
ADOBE EXPERIENCE
MANAGER FOR PURPOSES
OF IMAGING EFFICIENCY

Program Specialist (PS) James Greubel presented an oral and written report to the Committee on the Implementation of the Adobe Experience Manager for Purposes of Imaging Efficiency and discussed:

PROJECT RECAP & EXECUTIVE SUMMARY
PROCESS DISCOVERY FOR ERS
ROADMAP & RECOMMENDATIONS
DEMONSTRATION
ESTIMATED COST
NEXT STEPS

There was no action required of the Committee for this agenda item.

APPROVAL OF MINUTES
- JUNE 25, 2024

On a motion made by Vice Chair Barfield, seconded by Trustee Ley, and unanimously carried, the Committee approved the minutes of the June 25, 2024, meeting as presented.

PUBLIC COMMENT

Chair Chan called for public comment. There was no public present by teleconference or in person, therefore, no public comment.

(Chair Chan identified attendees of the Executive Session, Committee members Chair Chan, Vice Chair Barfield, and Trustee Ley, and ERS staff, Executive Director Thomas Williams, Chief Investment Officer Kristin Varela, Deputy Chief Investment Officer Anthony Goo, Chief Compliance Officer Kona Mann, Program Specialist James Greubel, Information Services Systems Supervisor Sandra Straub, Recording Secretary/Administrative Assistant Dale Kehau Kanae and Administrative Assistants Andrea Gasper and Lori Kim; Deputy Attorneys General Jenny Nakamoto, Lori Tanigawa, Elmira Tsang, and Diane Wong.

Chair Chan provided the reason to enter into Executive Session: Executive Session, pursuant to HRS §92-5(a)(4), (6), and (8), to consider and consult with the Board’s attorneys on questions and issues pertaining to the Board’s powers, duties, privileges, immunities, and liabilities, on information that must be kept confidential pursuant to State law, and to consider sensitive matters related to the Roadmap Report as part of the Internal Audit’s Virtual Chief Information Security Officer Project; an Update on the Implementation of ERS’ Compliance Program on Risk Assessment, Policies & Procedures, and Third-Party Risk

Management; an Update on Cyber Security; and to make a decision on the approval of Executive Session Minutes.)

ENTER EXECUTIVE SESSION

On a motion made by Trustee Ley, seconded by Vice Chair Barfield, and unanimously carried, the Committee entered into Executive Session at 2:48 p.m.

(Chair Chan requested, and all attendees confirmed, that no other persons were in their rooms or able to listen in on their audio or audiovisual connection while they were on the teleconference. Board Administrative Assistant Dale Kehau Kanae also confirmed that no unauthorized persons were in the conference room or able to listen in by audio or audiovisual connection while on the teleconference. Attendees are noted with an asterisk on these minutes and listed on the Executive Session Minutes.)

(Public participation concluded by ending the teleconference link.)

- Pursuant to HRS §92-5(a)(4), and (6), to consider and consult with the Board's attorneys on questions and issues pertaining to the Board's powers, duties, privileges, immunities, and liabilities, and to consider sensitive matters related to the Roadmap Report prepared as part of the Internal Audit's Virtual Chief Information Security Officer (vCISO) Project.
- Pursuant to HRS §92-5(a)(4) and (6), to consider and consult with the Board's attorneys on questions and issues pertaining to the Board's powers, duties, privileges, immunities, and liabilities, and to consider sensitive matters related to an Update on the Implementation of ERS' Compliance Program on Risk Assessment, Policies & Procedures, and Third-Party Risk Management.
- Pursuant to HRS §92-5(a)(4) and (6), to consider and consult with the Board's attorneys on questions and issues pertaining to the Board's powers, duties, privileges, immunities, and liabilities, and to consider sensitive matters related to Cyber Security Updates.
- Pursuant to HRS §92-5 (a)(8), to review and approve Executive Session Minutes of June 25, 2024.

EXECUTIVE SESSION, PURSUANT TO HRS §92-5(a)(4) AND (6), TO CONSIDER AND CONSULT WITH THE BOARD'S ATTORNEYS ON QUESTIONS AND ISSUES PERTAINING TO THE BOARD'S POWERS, DUTIES, PRIVILEGES, IMMUNITIES, AND LIABILITIES, AND TO CONSIDER SENSITIVE MATTERS RELATED TO THE ROADMAP REPORT PREPARED AS PART OF THE INTERNAL AUDIT'S VIRTUAL CHIEF INFORMATION SECURITY OFFICER (vCISO) PROJECT

EXECUTIVE SESSION, PURSUANT TO HRS §92-5(a)(4) AND (6), TO CONSIDER AND CONSULT WITH THE BOARD'S ATTORNEYS ON QUESTIONS AND ISSUES PERTAINING TO THE BOARD'S POWERS, DUTIES, PRIVILEGES, IMMUNITIES, AND LIABILITIES, AND TO CONSIDER SENSITIVE MATTERS RELATED TO AN UPDATE ON THE IMPLEMENTATION OF ERS'

COMPLIANCE PROGRAM ON RISK
ASSESSMENT, POLICIES &
PROCEDURES, AND THIRD-PARTY
RISK MANAGEMENT

EXECUTIVE SESSION, PURSUANT
TO HRS §92-5(a)(4) AND (6), TO
CONSIDER AND CONSULT WITH
THE BOARD'S ATTORNEYS ON
QUESTIONS AND ISSUES
PERTAINING TO THE BOARD'S
POWERS, DUTIES, PRIVILEGES,
IMMUNITIES, AND LIABILITIES,
AND TO CONSIDER SENSITIVE
MATTERS RELATED TO CYBER
SECURITY UPDATES

EXECUTIVE SESSION
PURSUANT TO HRS §92-5(a)(8),
TO REVIEW AND APPROVE
EXECUTIVE SESSION MINUTES
OF JUNE 25, 2024

EXIT EXECUTIVE SESSION

On a motion made by Vice Chair Barfield, seconded by Trustee Ley, and unanimously carried, the Committee exited Executive Session at 3:58 p.m.

Chair Chan announced that while in Executive Session, the Committee discussed matters related to the Roadmap Report as part of the Internal Audit's Virtual Chief Information Security Officer Project, an Update on the Implementation of ERS' Compliance Program on Risk Assessment, Policies & Procedures, and Third-Party Risk Management, matters related to Cyber Security Updates, and approval of the Executive Session Minutes of June 25, 2024.

ADJOURNMENT

On a motion made by Vice Chair Barfield, seconded by Trustee Ley, and unanimously carried, Chair Chan adjourned the meeting at 4:00 p.m.

REDACTED SIGNATURE

Thomas Williams
Executive Director

TW:dkik