Public Pension Funds

Operational Risks of Defined Benefit and Related Plans and Controls to Mitigate those Risks

Endorsed by:

Association of Public Pension Fund Auditors, Inc.

A Project of the Best Practices Committee

TABLE OF CONTENTS

FOREWORD

In July 2000, a group of public pension funds' chief investment officers and the Association of Public Pension Fund Auditors (APPFA) issued Public Pension Systems – Statements of Key Investment Risks and Common Practices to Address Those Risks. While much of the emphasis in public pension funds is on investment risks, the administrative and benefits (non-investment) side of public pension funds also face an extraordinary number of risks.

The Government Finance Officers Association (GFOA) subsequently requested that APPFA prepare a comparable document on benefit administration risks. In light of the broad acceptance and usefulness of the investment risk document by public pension funds nationwide, APPFA decided to look at non-investment risks. APPFA appointed a committee comprised of the following members to work on this project:

Richard Bendall, Co-Chair	Los Angeles County Retirement Association
Vicki Wickliffe, Co-Chair	Wisconsin Retirement System
Robert Benson	California Public Employees Retirement System
Jeanette Eckert	Louisiana State Employees Retirement System
Janet Harris	Public School Retirement System of Missouri
Jamie-Lyn Kinsella	North Dakota Public Employees Retirement System
Dennis Trzeciak	Ohio School Employees Retirement System

The first version of this publication was completed in July 2003 and was updated in February 2013 to include additional risks and controls related to public pension funds. The update was completed by the following members of the APPFA Best Practices Committee:

Flerida Rivera Alsing, Chair	State Board of Administration of Florida
Ryan Babin	Louisiana State Employees Retirement System
Amen Tam	Ontario Municipal Employees Retirement System
Toni Voglino	Maryland State Retirement Agency

The February 2013 version of this publication was approved by the APPFA Board in September 2013.

INTRODUCTION

Public pension funds (Funds) face a large number of risks on the administrative and benefits side of the business. Some inherent risks do not change much over time. However, other risks and the mitigating controls for all risks are often affected by the constant changes in technology and the environment in which the Funds operate. This publication lists some of the risks that Funds face and some of the controls that may be put in place to mitigate these risks.

This publication is intended to provide a point of reference or a guide to Funds' auditors, administrators, and others in addressing specific risks. It identifies key administrative risks and common practices to address, manage, and, to the extent possible, control those risks. Common practices may be appropriate for most Funds. However, an individual Fund's posture or resources might require lesser or greater actions, given the Fund's analysis of the potential impact of a particular risk and the cost of fully addressing that risk.

This publication does not address risks related to health insurance, life insurance, income continuation insurance, and other benefits that may be administered by third party administrators and does not address post-employment benefits not specifically listed in this publication.

This publication is not intended to be an exhaustive list of all risks that Funds may face on the administrative and benefits side of the business. Nor is it intended to be a comprehensive checklist of all the controls and other procedures a Fund should incorporate to address identified risks. The practices listed in this publication are common and proven approaches that may help Funds assess their approach to addressing similar issues. Common practices address common situations only. Examples in this publication may not be applicable to certain unique situations. The description of the key risks and possible actions discussed in this publication are intended as examples, not as standards or prescriptions.

We recognize that this publication might be used as a resource during periodic audits of Funds. If so, the auditor should keep in mind that this publication only describes existing common practices, not necessarily best practices. There are many ways to address the risks described. The primary consideration is whether the actions taken by the Fund mitigate the risk effectively, and not whether they follow the examples listed in this publication.

I. LEGISLATION/LEGAL ACTIONS/COURT DECISIONS

A. State Plans and Stand-Alone Local Agency Retirement Plans

1. Risks

- The public pension fund is not in compliance with existing federal/state laws
- Statutory language is difficult to interpret
- The plan is complicated, thus, expensive to administer and riskier
- Changes required by new municipal/federal/state laws or court decisions are not being implemented
- Legislators/government body(ies) enact laws/resolutions that negatively affect the public pension system
- Legislators/government body(ies) enact laws without the involvement of actuaries, Board of Trustees (Board), and/or public pension system management
- Legislative/government body(ies) actions present legal challenges to the public pension system
- Legislative/government body(ies) actions change pension benefits and contributions and materially impact funding
- Public pension system is not funded appropriately or consistently
- Implementation of new legislation is costly and new legislation may increase benefits without consideration of the additional costs or funding ability by the plan sponsor
- New legislation/ordinance/resolution requires large amount of time, has a tight implementation/compliance deadline, or cannot be implemented timely
- New legislation/ordinance/resolution cannot be implemented because of information technology constraints
- Individual employers pass ordinances or negotiate employment contracts that conflict with public pension system's statutes and rules
- Knowledge is not transferred to new legislators/plan sponsors when there is turnover in legislators/plan sponsors

2. Controls to mitigate the risks

- Provide a competent Board, good Board governance, competent staff, appropriate hiring practices, a competent legal office, and adequate legal staff
- Hire a competent Legislative Liaison to ensure the Board and management are aware of upcoming and pending legislative/government body(ies) actions
- Draft legislation/resolutions for consideration by the legislature/government body(ies)
- Prepare analyses and respond to legislative/government body(ies) initiatives

- Provide legislature/government body(ies) adequate information on the amount of time and money required to implement a proposed legislation/ordinance/resolution, including information technology constraints
- Participate in the orientation of new legislators/plan sponsors
- Perform employer audits
- Work with appropriate associations to educate employers about new and pending legislation/ordinance/resolution

B. Local Public Agency Plans Contracting with a Public Pension Fund

1. Risks

- Contract with public agency does not conform with existing federal/state laws
- New local ordinances and Memoranda of Understanding (MOUs) conflict with applicable state laws and regulations
- Eligible public agency is rejected or an ineligible entity is accepted
- Employment contracts are not in compliance with laws or regulations
- Contracted benefits with public agencies are diverse and complicated, making the system expensive to administer and riskier
- Individual employer risk pools are so small and pose a risk to individual public agencies and/or local taxpayers
- Plan contract does not incorporate changes required by new federal/state laws or court decisions
- Staff turn-over of benefit officers at public agencies adversely affects communications with both the employer and the members

2. Controls to mitigate the risks

- Require a legal review of contracts to ensure compliance with existing federal/state laws. Ensure contracts have provisions for, or are amended appropriately for, changes in federal/state laws
- Inform and educate public agencies on applicable laws and regulations
- Provide ongoing training to benefit staff at the public agencies or have pension staff complete the training
- See list of controls to mitigate the risks in *section I.A, State Plans and Stand-Alone Local Agency Retirement Plans*

II. ADMINISTRATION

A. Board of Trustees (Board)

1. Risks

- Board members are not adequately trained and qualified to perform their functions and fiduciary responsibilities
- Board members do not meet frequently enough to perform their functions and fiduciary responsibilities
- Board members do not have expertise to promulgate policies for a public pension system
- Board members do not select qualified executives
- Board members micro-manage the public pension system
- One or more Board members may not be independent and/or may have a conflict of interest and/or may not be performing their fiduciary duties
- Board members are not provided sufficient and timely information by public pension system executives in order to make informed decisions

2. Controls to mitigate the risks

- Complete background checks prior to appointment or election of board members
- Provide orientation and training to new Board members
- Conduct or provide continuing education to Board members. Develop list of approved conferences or Continuing Professional Education providers
- Develop bylaws or Board charter which includes detailed duties of each officer and committee, including fiduciary requirements.
- Develop an Ethics Policy for Board members
- Require Board members to complete a financial disclosure/conflict of interest statement annually
- Outline the frequency of meetings in the Board charter
- Send meeting materials to Board members at least a week before the meeting
- Hire a Board Coordinator to coordinate Board activities and ensure that Board members receive appropriate information timely
- Conduct or have a periodic fiduciary audit
- Promulgate rules for the qualifications, selection, and retention of the public pension system's executive team

B. Audit Committee

1. Risks

- There is no Audit Committee

- Audit Committee members are not adequately trained and qualified to perform their functions and fiduciary responsibilities
- Audit Committee members are not aware of their fiduciary responsibilities
- Audit Committee is not adequately involved in the selection of external auditors and does not have adequate communications with external auditors
- Audit Committee does not adequately assess the independence of external auditors
- Audit Committee has inadequate interaction with the internal audit function; no or little involvement in the selection of the Chief Audit Executive, approval of the internal audit plan, etc.
- One or more Audit Committee members may have a conflict of interest

2. Controls to mitigate the risks

- Establish an Audit Committee
- Develop an Audit Committee charter to establish authority and responsibilities
- Develop an annual Audit Committee work plan
- Run background checks prior to selecting Audit Committee members
- Require Audit Committee members to complete a financial disclosure/conflict of interest statement annually
- Provide orientation and training to new Audit Committee members
- Provide continuing education to all Audit Committee members
- Send meeting materials to Audit Committee at least a week before the meeting
- Ensure that internal and external auditors have direct and sufficient access to the Audit Committee

C. Executive

1. Risks

- Executives do not have management and technical skills to manage the system
- Executives are engaged in inappropriate activities such as criminal activity, unethical conduct, and fraudulent activity, before and/or during employment
- Executives do not perform their fiduciary duties
- The public pension system gets involved in many inconsequential projects, causing critical functions to suffer
- One or more executives may have a conflict of interest

2. Controls to mitigate the risks

- Develop appropriate hiring practices, including adequate job descriptions and minimum qualifications

- Conduct detailed background checks before hiring, including applicant's identity, education, employment history, current or most recent employment, criminal history, and personal references
- Provide adequate training and education on management functions, responsibilities and accountability
- Provide executives training on internal controls, such as appropriate separation of duties, oversight, etc.
- Provide executives appropriate technical training
- Adopt a code of conduct
- Require executives to complete annual financial disclosure/conflict of interest statement that is subject to periodic audit
- Conduct a performance review annually
- Require managers to perform an annual internal control review, implement appropriate controls to mitigate identified risks, and establish appropriate monitoring/oversight activities
- Ensure that internal audit function reports directly to Audit Committee or the Board

D. Strategic Planning

1. Risks

- Public pension system neither plans adequately nor documents its mission statement, strategic plan, implementation plans, charters, and policies and procedures for all areas (including the Board, its Committees, and each program area)
- Major projects fail or are not completed timely due to inadequate planning
- Public pension system doesn't adequately manage and monitor materials risks or threats to the plan
- Staff resources are not allocated appropriately and efficiently

2. Controls to mitigate the risks

- Develop and monitor organization-wide mission statement, strategic plan, and short-term plans and goals
- Appoint a Planning Director whose responsibilities include development of a mission statement, strategic plan, and coordination of the implementation plans
- Perform an annual risk assessment (not to be confused with the internal audit annual risk assessment) to identify risks and determine priorities
- Provide executive oversight team(s) to sponsor, monitor, and prioritize major projects
- Provide knowledgeable staff to plan, test, implement, document, and monitor major projects

- Document procedures on all repetitive processes performed by public pension system staff
- Appoint an employee who will coordinate written processes among various segments of the organization
- Monitor processes and procedures to ensure compliance with mission statement and strategic plan

III. STAFFING

A. Recruit, Develop and Retain High Caliber Employees

1. Risks

- Public pension system does not offer sufficient salaries, benefits, and appropriate working environment to attract and retain high-caliber employees
- Adequate formal and on-the-job training is not provided
- Employees do not have the knowledge or expertise for the position
- Hiring criteria or standards are not met because individuals with falsified previous employment, education or other relevant information are hired
- Employees are engaged in inappropriate activities such as criminal activity, unethical conduct, and fraudulent activities before and/or during employment
- Employees are not encouraged nor provided the opportunity to acquire skills for higher level positions
- Employees are not encouraged to participate in professional societies and to obtain professional certifications where appropriate2. Controls to mitigate the risks
- Conduct periodic salary/benefit surveys to ensure the public pension system is competitive in the job market. Surveys should include a review of the local, regional, and national markets
- Provide adequate orientation to new employees, including information on the public pension system's ethics, values and code of conduct. Indicate and pursue penalties for violations or non-compliance
- Provide employee handbooks that include job descriptions, organizational charts, compensation and leave policy, and descriptions of benefits
- Conduct annual/periodic employee evaluations
- Develop, administer, and/or promote a training plan for all staff
- Provide adequate funding for staff training
- Provide adequate training to new employees and periodic training to other employees
- Offer training and/or mentoring to prepare employees for higher level positions
- Encourage participation in professional societies by paying dues and offering time to attend meetings, serve on society boards, and travel to meetings
- Encourage professional certifications by paying for examination fees and study materials and offering time to prepare for exams
- Encourage maintenance of professional certifications by paying annual dues and pay for the continuing professional educational requirements
- Establish a robust pre-employment screening process

- Conduct thorough background checks on individuals being considered for employment or promotion to a position of trust, especially for those who have high level access authority to member records. Background check should include applicant's identity, education, employment history, current or most recent employment, criminal history, and personal references
- Develop appropriate hiring practices, including job description/minimum qualifications
- Establish mentoring program

B. Managing Employees

1. Risks

- Public pension system managers do not properly manage their employees
- Agency divisions do not function in harmony with each other
- Management and board directives are not communicated to staff
- Work is not performed consistently
- New employees receive insufficient guidance
- There is no continuity during employee turnover, leave, and/or reassignment
- Employees have a conflict of interest
- Job functions are not clearly defined and communicated to staff
- Employee evaluations are not done timely and/or meaningful
- Staff lack integrity and ethics

2. Controls to mitigate the risks

- Ensure careful selection of managers
- Offer management training to new managers and management skills refresher classes to existing managers
- Encourage management meetings to discuss cross-divisional issues. Take meeting minutes and publish to document decisions and discussions
- Encourage communication among all work areas
- Involve staff in major projects to obtain their perspective
- Appoint or hire an individual to coordinate cross-divisional communication and solutions to enterprise problems, or train existing managers in these skills
- Develop written procedures for all repetitive processes and update them timely to ensure management and Board directives are communicated to staff and work is performed consistently. Written procedures save time, especially when training new employees, and provide continuity during employee turnover, leave, reassignment, and /or during a business interruption (disaster)
- Document intra-departmental administrative decisions

- Update written procedures for administrative decisions that impact permanent changes in processing
- Provide clear and current job descriptions for employees
- Prepare and review performance evaluations timely
- Adopt a code of conduct and include it in the employee handbook
- Require employees to sign code of conduct statement annually; follow up non-replies
- Set the tone at the top for a culture of honesty and ethics. Clearly communicate to staff acceptable behavior and expectations
- Provide periodic training to all employees on the public pension system's values and code of conduct
- Create a positive workplace environment by providing timely feedback, employee recognition, reasonable expectations, etc.
- Provide for a telephone hotline or whistle blower contact to encourage employees to report actual or suspected wrongdoing or potential violations of the code of conduct
- Immediately address violations to the public pension system's ethics, values and code of conduct
- Establish guidelines and controls regarding outside employment

C. Segregation of Duties

1. Risks

- Public pension system does not properly segregate duties among its employees
- Compensating controls do not adequately mitigate risks in areas where segregation of duties is not sufficiently possible
- Segregation of duties is overridden

2. Control to mitigate the risks

- Require division managers and staff to conduct annual or periodic self-assessment
- Provide training to management on proper segregation of duties
- Request internal audit to review segregation of duties in high risk areas

IV. ENROLLMENT OF MEMBERS

1. Risks

- Eligible employees are not enrolled
- Ineligible employees are enrolled
- Ghost employees are enrolled
- Employees are enrolled in an incorrect employment category, tier, or pension plan, either intentionally or unintentionally

2. Controls to mitigate the risks

- Provide education or training sessions to employers
- Distribute employer administration manual to all employers
- Communicate to employers changes or issues affecting member eligibility
- Provide standardized enrollment forms which require completion of all information necessary to determine eligibility
- Provide on-line, self-editing enrollment where computer feeds back incorrect entries
- Perform computer matches between enrollment data and payroll data
- Require employers to post employee benefits and pension plan eligibility rules
- Require internal audit to conduct periodic audits of employer payrolls
- Provide some type of validation of employment status and employment category

V. COLLECTION AND MAINTENANCE OF MEMBER DATA

A. Enrollment Data

1. Risks

- An incorrect benefit formula is associated with a member
- Name on Social Security card is not required on employment records, as required by Internal Revenue Service (IRS) Publication 15, Circular E
- Incorrect birth date is received and/or recorded
- A member may intentionally or mistakenly misrepresent their age and receive retirement benefits before they are actually eligible
- Incorrect marital status is received and/or recorded
- Correct beneficiaries are not recorded
- Beneficiary splits are not recorded correctly
- Correct address is not received and/or recorded
- Person reporting the change of address is not authenticated
- No integrated address system to assure addresses are consistent
- Incorrect Social Security Number (SSN) is received and/or recorded
- IRS fines public pension system for using incorrect SSN
- Incorrect gender is entered into the system, affecting actuarial calculations

2. Controls to mitigate the risks

- Develop adequate written procedures and guidelines for staff
- Include reference to the member's benefit formula in member statements
- Require a copy of Social Security card for member file or completed IRS Form W-9
- Use the Social Security Administration's (SSA) Employee Verification System to identify name discrepancies, inaccurate SSN, gender, etc.
- Verify keyed SSNs using techniques such as duplicate keying
- Require same name on both SSA and public pension system's records
- Require copies of all marriage licenses
- Require copies of all divorce decrees
- Require copies of divorce settlements
- Require awareness of community property provisions in state laws (some states only)
- List beneficiaries and note percentage splits on annual statement of benefits
- Send confirmation letter (communication) to member for any address change
- Follow-up timely mails returned as undeliverable

- Have a procedure for authenticating changes of address (signatures, passwords, voice identification, questions that only the member would know)
- Implement an integrated address system

B. Payroll Data

1. Risks

- Incorrect compensation/contribution data is received and/or recorded
- Contributions are not correct because of wrong contribution rates, incorrect data, and/or incorrect calculations
- Reported compensation includes earnings that are not retirement eligible (such as overtime, per diem, etc.)
- An agency is paying contributions on ineligible earnings
- Retroactive payments are not handled correctly
- Contributions received are not credited to the correct accounts
- Public pension system applies incorrect interest rates when collecting contributions from different fiscal/calendar years
- Employer does not update programs for contribution changes, thus submitting inaccurate information
- Payment for employer and/or member contributions are incorrect
- Payroll data is not received timely or at all
- Public pension system staff does not follow up on contributions not received
- Payroll data is not recorded promptly into the member database, resulting in erroneous benefit calculations which must be updated
- Incorrect service credit data is received and/or recorded
- Employer incorrectly reports tax deferred contributions as regular taxable contributions or reports regular taxable contributions as tax deferred contributions
- Employer does not notify the public pension system of changes to tax deferred contributions in a timely manner
- Tax deferred contributions are not included as salary for retirement purposes
- Computer system edits are not sufficient and allow posting of inaccurate information to member records
- Web submission of the agency's wage and contribution report does not have adequate validation checks to prevent the agency from sending incorrect information

2. Controls to mitigate the risks

- Suggest that internal audit conducts audits of individual employers

- Provide employer training
- Develop and distribute employer administration manuals that include examples of reportable and non-reportable earnings, examples of differences between reporting criteria for retirement system and other governmental agencies such as IRS and SSA, and information on the importance of documenting decisions involving earnings
- Send periodic employer newsletters and bulletins
- Promulgate administrative rules to clarify statutory provisions for reportable earnings
- Develop a website for employer information and questions
- Create a system that receives data promptly and records information into each member's account in a timely manner
- Include transaction documentation/audit trail in participant files for each monetary adjustment
- Reconcile bank account receipts to employer payroll reports received to ensure all the payroll contributions due equal the corresponding receipts
- Match contribution rates paid with contribution rates required by actuaries
- Send quarterly statements to employers listing employer and member contributions received by the plan, and employer beginning and ending account balances so that employers can reconcile their books to public pension system books
- Create an Employer Self Audit process that allows employers to check their own data
- Maintain a list of anticipated employer payroll reports and check them off as received
- Follow-up on payroll reports not received
- Implement statutes and/or rules that penalize employers for submitting late reports or receipts
- Conduct a review to determine that contributions are paid based only on retirement eligible wages
- Perform evaluations and inform the employer promptly of changes in employer contribution rates; provide explanation of the changes
- Validate contributions independently to assure rates are accurate
- Review computer system edits and validation checks periodically
- Have an upfront control validations such as limit checks on calculated amounts, table lookups, check digits (to help identify transposition or key punch errors). These validations should be performed prior to submission by employer

agencies. A log should keep track of the process of submitting contributions via the web

C. Changes to Member/Retiree Data

1. Risks

- Incorrect and/or unauthorized changes are made to name, address, SSN, date of birth, and other indicative data
- Members do not give timely notification of change
- Data is inconsistent between stand-alone systems or among data components of integrated systems
- Paper documents are not stored securely before being imaged
- Fund is maintaining paper documents rather than digital documents
- Sensitive/confidential documents are not properly safeguarded and disposed of when no longer needed
- Changes in employment are not received and/or recorded
- Changes in marital status, divorce court settlements, and community property agreements are not received and/or recorded properly and timely
- Changes in beneficiaries are not received and/or recorded timely or accurately
- Unauthorized changes are made to beneficiary information
- Child support orders are not received and/or recorded properly and timely
- Unauthorized changes are made to member data
- Employees who are members have improper access to their own files/data
- Employee changes information on the system on a member who is a relative or a friend of the employee

2. Controls to mitigate the risks

- Develop procedures for authenticating source(s) of changes in member data including but not limited to, comparison of signatures, passwords, and digital signatures
- Develop written procedures to ensure compliance with relevant statutes and consistent/accurate processing and performance standards
- Develop written policies and procedures for disposal of documents no longer needed
- Use SSA's Employee Verification System to identify/correct inaccurate indicative data
- Send confirmation letters to member when beneficiaries are changed
- Have an automated system to track any changes to a member's record and record the date and user making the change

- Monitor member records for unusual items or changes
- Allow system or subsystem or module access only to staff needing access for their jobs
- Send annual statements with request to members to notify the public pension system if data is incorrect
- Establish a post-processing reconciliation review of all participant account information
- Include transaction documentation in participant files for each service adjustment to provide an audit trail
- Follow-up timely on any mails returned as undeliverable
- Have a procedure for authenticating changes of address (signatures, passwords, voice identification, questions that only the member would know)
- Publish a brochure such as "How Divorce Can Affect Your Benefits," and emphasize the importance of having a current beneficiary designation on file
- Send a new beneficiary designation form to members and annuitants after receipt of documentation and/or court orders indicating divorce
- Develop a periodic process for sampling and testing file maintenance transactions
- Reconcile data between stand-alone systems
- Use automated validation techniques to reconcile data components of integrated systems
- Store documents securely until imaged

D. Maintenance of Member/Retiree Data

1. Risks

- Data is not maintained and backed up properly to maintain data integrity
- Database is not secure from both internal and external threats, compromising data confidentiality
- Electronic data is lost because of system outages
- Data is not accurate
- Data exceptions/errors are not identified and/or corrected on a timely basis
- Paper files/records are not secure from fire or other natural disasters
- Member records are used unethically or illegally by public pension system staff
- Member files (paper) are not complete
- Member files (imaged) are not complete and are not properly backed up
- Member imaged files cannot be accessed timely when the system is down
- Fund has not established a procedure for guarding sensitive information and reducing the potential for identity theft

2. Controls to mitigate the risks

- Ensure physical security of the premises and of the information system components
- Ensure logical security for the information system components
- Conduct security awareness training for employees
- Change user identification and passwords periodically, such as every 60-90 days
- Back up data daily
- Develop written policies and procedures to ensure compliance for daily back-up of data
- Store data in a secure manner
- Review confidentiality policy of employees on annual basis and update as necessary
- Review system accessibility by all staff members periodically and allow system access only for staff needing access for their jobs
- Use SSA's Employee Verification System to identify/correct inaccurate data
- Send annual statement of account to members with dollar amounts, date of birth, beneficiary, etc. so that member has opportunity to identify data errors
- Use system generated identification number rather than SSN on correspondence to reduce potential for identify theft
- Develop a business continuity/contingency plan and tests of the plan, including a back-up business resumption site
- Establish information technology (IT) security controls, including monitoring home access (remote) and monitoring what files are accessed
- Allow sufficient time to correct identified problems and locate forms before destroying records for a new imaging system
- Microfilm critical records and store microfilm off-site
- Develop written administrative policies, criteria, and procedures for record retention
- Research or test longevity of medium/systems used if record is supposed to be permanent/historical

VI. COMMUNICATIONS WITH MEMBERS

A. Enrollment

1. Risks

- New members do not receive adequate information about the public pension system
- Public pension system's counselors are not adequately trained
- Employer benefit specialists are not adequately trained
- Information provided to members is not accurate, clear, consistent or timely, thereby adversely affecting member decisions

2. Controls to mitigate the risks

- Develop a summary plan description (SPD) that completely, accurately, and clearly describes the significant features of the public pension system (Government Finance Officers Association (GFOA) recommended practice)
- Conduct orientation sessions for new employees
- Offer training, materials, and refresher classes for employer benefit specialists
- Provide adequate initial and ongoing training to public pension system's counselors
- Send periodic member newsletters
- Include new member information on public pension system's website
- Provide employers educational materials and tools which facilitate the transfer of information on the pension fund to each new employee
- Develop a thorough review process for publications and forms prior to release to employer agencies and members
- Offer educational outreach for members (such as retirement video)

B. Member Statements

1. Risks

- Member statements are inaccurate and/or incomplete
- Members do not receive statements
- Someone other than the member receives the statement

2. Controls to mitigate the risks

- Perform a quality control check for a sample of statements
- Provide a way for members to correct inaccurate information via mail, telephone, or website after proper authentication
- Use an abbreviated rather than the full SSN on the statement

- Use the United States Postal Service Annual Address Match
- Use an online service to locate lost contacts

C. Retirement Estimates

1. Risks

- Estimates are provided to a member before service credit history has been recorded and/or audited
- Retirement estimates are not accurate because of incorrect and/or incomplete information:
  - Benefit formula
  - Option
  - Employment category
  - Service credit
  - Final compensation
  - Age at retirement

2. Controls to mitigate the risks

- Periodically test the system with data for which the outcome is known
- Provide quality assurance review of calculated estimates
- Create a system that receives data promptly and records information into the member database promptly (*see section V, Collection and Maintenance of Member Data)*

D. Retirement Planning Services

1. Risks

- Members do not receive adequate retirement planning services
- Retirement alternatives are not adequately presented to potential retirees
- Staff providing services are not well trained and provide incorrect information to potential retirees

2. Controls to mitigate the risks

- Provide periodic financial education and retirement planning sessions throughout the employees' careers (GFOA recommended practice)
- Offer pre-retirement planning sessions at least 5 years prior to projected retirement age (GFOA recommended practice)
- Provide a well-designed, ongoing training program to retirement staff
- Provide well-designed, up-to-date, and easily understood information on the website

E. Customer Service

1. Risks

- Various forms/methods of communication with members, retirees, and beneficiaries are neither coordinated nor consistent (i.e., literature, internet, telephone, and field offices)
- Public pension system communication, processes, and policies are not customer oriented
- Appeals/disputes occur because of inadequate communication among members, employers, the public pension system, and third party administrators
- Employer benefit specialists are not given adequate information and training to communicate pension plan provisions to employees

2. Controls to mitigate the risks

- Appoint or hire an Information/Communication Coordinator for the public pension system
- Appoint or hire a Manager of Quality Assurance and/or form a Quality Assurance Committee
- Develop an ongoing quality assurance process involving closed appeals and a continuous review of possible improvements in customer service, policies, processes, forms, and communications
- Participate in a study to measure performance and cost effectiveness to learn how comparable public pension systems perform; develop new service standards; identify best practices; monitor performance; identify priorities; identify areas needing improvement; better understand the system; improve the decision-making process; and implement changes to improve the quality of customer service

F. Publications

1. Risks

- Literature available to members is incomplete/inaccurate
- Newsletters and special mailings are unclear
- Standard publications are not consistently used to provide accurate information to large groups
- Information in publications does not agree with statutes, rules, or contract
- Forms cannot be kept up-to-date and inventoried because of the volume

2. Controls to mitigate the risks

- Have appropriate staff and/or the legal office review and sign off on new/revised forms and publications
- Enlist the assistance of annuitants and/or external employees to review important mailings before they are sent
- Appoint or hire a forms coordinator to coordinate forms for the public pension system
- Note revision dates or expiration dates on forms
- Include appropriate language on publications such as: "Every effort has been made to ensure that the information in this publication is accurate. If the information should conflict with the law, rules, contract, or plan language, then the law, rules, contract or plan language must take precedence."
- Review the summary plan description (SPD) periodically to keep it current (GFOA recommended practice)

G. Internet Access to Information

1. Risks

- Information made available on the Internet does not agree with statutes, rules, or contracts
- Information on the Internet is incomplete/inaccurate
- Access to individual's private information is not secure
- Customers are not authenticated prior to accessing confidential information or providing confidential information
- Members use website to make decisions on their retirement and the information provided to them is incorrect or they make incorrect assumptions based on the data to their detriment

2. Controls to mitigate the risks

- Develop procedures for appropriate staff and/or the legal office to validate/review information prior to placement on the website (review and sign-off)
- Have qualified staff check existing information on the website on a set periodic basis
- Maintain physical security and logical security of website and data
- Authenticate users (for example, require pin numbers to access member account via the internet)
- Provide appropriate education and training to staff working on website

- Assign one or more individuals the responsibility for maintaining the website timely
- Include appropriate language on the website such as: "Every effort has been made to ensure that the information on this website is accurate. If the information should conflict with the law, rules, contract, or plan language, then the law, rules, contract or plan language must take precedence."
- Include a disclaimer on the website upon login which warns the member to not rely totally on the information

H. Customer Call Center

1. Risks

- Information made available does not agree with statutes, rules or contracts
- Information given by call center is incomplete/inaccurate
- Call center employees are not adequately trained
- Callers are not authenticated and confidential information is given or customer information is accepted
- Call center staff do not provide information timely
- Calls are not answered or required to hold for a long period of time

2. Controls to mitigate the risks

- Have appropriate staff and/or the legal office review information made available
- Provide ongoing training and supervision to call center employees, using approved information
- Develop a training manual to train call center employees
- Update other resources, such as keyword searchable database of frequently asked questions (FAQs), to answer callers' questions consistently and accurately
- Use experienced staff as resources and mentors
- Authenticate caller identity at the beginning of each call. Establish standardized questions to identify member before releasing or accepting confidential information
- Record calls to use as training tools and to identify problem issues, using established benchmarks
- Install and maintain the telephone system properly
- Establish a service level objective to answer calls within a certain period of time and monitor the call response times

I. Field Offices/Field Presentations

1. Risks

- Information does not agree with statutes, rules, or contracts
- Information is inaccurate and/or incomplete
- Field offices/presentations are not easily accessible to members, retirees, and beneficiaries
- Field staff do not receive adequate formal and on-the-job training
- Customers are not authenticated before confidential information is given or customer information is accepted

2. Controls to mitigate the risks

- Have appropriate staff and/or the legal office review and sign off on available information
- Set up permanent or temporary satellite offices throughout the region
- Conduct employee benefit presentations regularly throughout the state
- Provide adequate initial and ongoing training for field office staff
- Authenticate customers at the beginning of the session

J. Unclaimed Member Accounts and Unclaimed Benefits

1. Risks

- Public pension system does not comply with IRS minimum distribution requirements
- Inactive members who are deceased are not identified
- System does not effectively pursue contact with lost retirees and/or beneficiaries
- Public pension system does not adequately search for inactive members
- Public pension system does not provide a mechanism whereby inactive members or heirs of inactive members/annuitants can search for unclaimed benefits
- Public pension system staff divert unclaimed funds for their own personal use
- Someone steals member's identity and fraudulently claims the account
- Poor public perception results when locator services independently find published lost contact members and charge members a high percentage fee

2. Controls to mitigate the risks

- Identify inactive records with a special code
- Review inactive accounts for compliance with IRS minimum distribution requirements
- Use on-line search services, locator services, and/or National Change of Address Service

- Match data with files maintained by other federal/state agencies/divisions such as Office of Vital Records, Division of Motor Vehicles, Department of Revenue, State Treasurer, Division of Unemployment Compensation, and IRS to identify/correct inaccurate data
- Contact former employers for addresses of inactive/terminated members
- Publish annually a list of unclaimed accounts and/or benefits in the official state newspaper and public pension system newsletter
- List lost members and retirees on internet site
- Use SSA's Employee Verification System to identify/correct inaccurate data, thus improving capability of locating member, identifying a death, or making automatic distributions timely
- Attempt to contact inactive employees prior to the year in which IRS requires minimum distribution
- Use SSA Death Master File to identify deceased inactive participants
- Require addresses from all employees and employers at termination
- Stratify inactive member balances so higher risk (dollar) accounts receive priority
- Periodically send Statement of Account or newsletter to inactive members
- Follow up timely Statements of Account returned as undeliverable
- Ensure that state statutes provide criteria for identifying lost contacts, publishing names, and writing off or paying amounts
- Develop additional controls such as supervisory reviews and required birth evidence when paying benefits on accounts that have been inactive for a period of time
- Establish controls related to the completion of retirement applications, such as notarized applications, to deter internal employees from filing for unclaimed retirement benefits
- Match retiree addresses to internal employee address to locate employee that may have filed for an unclaimed retirement benefit

K. Form 1099-R and 1042-S

1. Risks

- 1099-R form is incorrectly generated for someone who should not receive one or not generated for someone who should receive one
- Plan for processing 1099-R and 1042-S forms are not established by management
- Incorrect information is populated on the 1099-R or 1042-S forms
- 1099-R or 1042-S forms will not be issued to recipients by the January 31st deadline

- All "return to sender" 1099-R and 1042-S forms are not researched and reissued
- In instances when the IRS instructions are unclear, assumptions made by staff are not reviewed by specialized tax counsel to ensure compliance with IRS rules and regulations.
- File not provided to IRS in an accurate and timely manner
- 1099-R form issued instead of 1042-S form (foreign)

2. Controls to mitigate the risks

- Develop detailed written procedures for processing 1099-R and 1042-S forms
- Thorough testing of the 1099-R and 1042-S data and forms should be performed prior to being issued
- Plan and create a checklist to facilitate the completion of the 1099-R and 1042-S process timely and effectively
- In instances when the IRS instructions are unclear, have all tax related assumptions submitted to specialized tax counsel for review and clarification

VII. ALL BENEFITS

1. Risks

- Benefit amount is incorrectly calculated because of:
  - incomplete/inaccurate data, service credit, and/or final compensation
  - incorrect benefit formula
  - system errors
  - human errors
  - incorrect birth date (age at retirement)
  - incorrect leave balance (i.e., accrued vacation or sick leave)
  - benefit changes over time that must be manually calculated
- Benefits are paid to unauthorized persons
- Inactive claimants are not properly authenticated before payment is made
- Benefit is fictitious or not authorized
- Benefits are paid to deceased persons
- Mortality tables are not updated when appropriate
- Benefit calculation errors are not discovered
- Underpayments due members/retirees are not subsequently paid
- Overpayments to retirees/beneficiaries are not subsequently collected per applicable statutes
- Benefits are not paid timely
- Paper checks are lost or not received timely
- Payments are not in compliance with IRS regulations for automatic distributions
- Unauthorized benefit payments are calculated and paid
- Duplicate payments are made
- Unclaimed benefits are not properly recorded, accounted for and safeguarded
- Stale dated checks are not followed up on
- Stale dated checks are automatically reissued without follow-up, resulting in payments to deceased persons
- Stale dated checks are automatically reissued without adequate segregation of duties, resulting in diversion of checks by public pension system staff for their own use
- An employee is allowed to work on calculations of a relative or friend
- Employees intentionally alter a claim in the computer system, resulting in overpaid benefits
- Exceptions are not identified and followed up on
- Federal/state tax withholding amounts are incorrect or are not adjusted as conditions change

- Incorrect SSN is sent to federal/state tax authorities
- Benefit enhancements are not provided timely or accurately
- Identity theft results in fraudulent payments
- Inappropriate deductions are taken from benefit payments (for example, dissolution orders, wage assignments, and elective deductions such as savings bonds or credit unions)

2. Controls to mitigate the risks

- Develop written policies and procedures to ensure that benefits are processed accurately, uniformly, and timely in compliance with state statutory provisions, administrative rules, IRS requirements, and management directives
- Create an on-line desk manual
- Document processes for any special rules that may apply to manual calculations
- Provide retiree with summary of data used in benefit calculation, including benefit formula, service credit, highest/average compensation, age, gender, calculation(s)
- Provide adequate segregation of duties among staff processing benefits, including reissuing stale-dated checks
- Authenticate person requesting a benefit
- Require notarized signatures on applications from persons who have been inactive for a period of time
- Require additional documentation (such as SSN card or birth certificate, if not already on file) from members who have been inactive for a specific period of time
- Require supervisory reviews of benefits paid on accounts that have been inactive for a specific period of time
- Conduct death matches for annuitants/non-annuitants using SSA Death Master Death File/updates, state Vital Records, and/or outside vendors
- Send confirmation letters to persons who are listed as deceased on death match reports and require a (notarized) signature before making payment to applicants or continuing monthly benefits to annuitants
- Record dates of death on member records immediately
- Use SSA's Employee Verification System to identify/correct inaccurate SSNs, names, and dates of birth, thus improving the accuracy of death matches, benefit calculations, and benefit payments
- Require copy of birth evidence and Social Security card for member's file
- Generate exception reports and conduct regular supervisory reviews of them
- Establish performance standards for timeliness and accuracy

- Require/encourage electronic payments to banks
- Develop charts and/or checklists to aid staff in determining benefits payable
- Update mortality tables periodically (for example, every 5 years) (*see section XIII, Actuary*)
- Test automated benefit calculations adequately
- Send annual statement of benefits to inactive members
- Notify inactive members of minimum distribution requirements prior to the year in which IRS requires distribution
- Use restricted delivery for certified letters when sending benefit information about IRS minimum distribution requirements to inactive members
- Publish annual article in system newsletter, emphasizing the tax penalty and the importance of complying with IRS minimum distribution requirements
- Develop written procedures for following up on un-cashed checks
- Verify that payee is alive before reissuing a stale-dated check
- Utilize computed assisted audit techniques (CAAT) to test benefit calculations
- Develop a well-controlled account receivable process
- Use a collection agency to recover overpayments that are difficult to collect
- Publicize litigation against those who fraudulently received benefits
- Conduct identity theft training for applicable staff
- Examine transit routing and account numbers periodically where multiple checks are being electronically routed
- Verify that inactive member is living before contacting and/or making automatic distributions
- Use automated edits/matches to identify invalid/incorrect SSNs for pending payments
- Use a separate post office box and independent pick-up for checks returned as undeliverable or establish a central place for receipt of returned checks
- Reconcile benefits processed/paid with statistics for various work areas
- Print following language on checks: "void if payee died prior to check date"
- Reconcile employee and employer accounts on a monthly or more frequent basis
- Perform analytical audits and make year by year comparisons of member account values to detect abnormal changes between years

VIII. WITHDRAWALS/REFUNDS

1. Risks

- Refund is made to the wrong person
- An incorrect amount is paid
- A transferee from one agency to another receives a refund in error
- Payee cannot be located if supplemental benefit is to be paid
- Taxes are not withheld if contributions are not rolled over to qualified plan
- Records are not retained long enough after payment and data is needed if person re-enrolls
- Member contributions and service credit are not reduced to zero after refund
- Accounts of active members who died while active are not researched and resolved timely, either by paying the survivor benefit or by refunding
- An overpayment of refund could be made due to a credit taken by an agency
- Refund forms are not entered into the system as they are received
- Refund forms are not reviewed for completeness (e.g. certified and signed by the Payroll department)
- Refund payments are not made according to statutes and/or policies
- Someone steals member's identity and fraudulently claims the account
- Application data is not accurate resulting in ineligible members receiving refunds or other refund errors
- Application processing is not completed timely
- Data in member record is inaccurate, resulting in erroneously calculated refunds
- Refund applications are lost or misplaced, delaying refund processing
- Refund expenditures are not appropriately identified and posted to accounting records
- Staff fraudulently issues a refund payment for personal gain
- Employer certifies incorrect member contributions for current year on the refund

2. Controls to mitigate the risks

- Authenticate persons requesting refunds
- Maintain up-to-date and accurate member records (*see section V, Collection and Maintenance of Member Data*)
- Inform members of withholding requirements if money is not transferred to qualified plan through the brochures, Internet, on the telephone, and at the time of the request to withdraw the member contributions
- Retain records for extended period of time based upon state law and life expectancy

- Refund form must be submitted and approved before payment is released
- All new claims and adjustments should be reviewed and authorized by someone other than the staff processing the claim
- Check each application for completeness and verify the application and supporting record for accuracy
- Provide a refund application form and instructions
- Generate and review a daily report of refunds to ensure all applications are properly processed
- Generate and review a preliminary refund report for each refund payroll
- Refund amounts are calculated by computer application that takes into account calculation rules
- Develop verification steps to help ensure basic calculation inputs are correct
- Require adequate identity documentation when an individual is refunded
- Require supervisory review and approval of each refund prior to payment

IX. DISABILITY RETIREMENT BENEFITS AND ESTIMATES

1. Risks

- A person is not truly disabled under the provisions of law/contract
- Physicians are paid for services they did not perform or are paid twice for the same services
- Public pension system has no checks/balances on effectiveness of physicians who evaluate applicants/recipients
- Physicians performing medical exams are not qualified/independent of member
- Access to confidential medical information is not restricted as required by law
- Disability applications are not reviewed for statutory timing constraints
- Application is not processed within a reasonable period of time
- Continuing eligibility is not verified
- Benefit is not stopped once the System/Board determines that an individual is not disabled
- Benefit is not offset for applicable income or is not offset timely
- Allowable earnings are not independently verified when disability recipient is gainfully employed (in Funds with allowable earnings limitations)
- Disability recipients who have reached the age for regular retirement (and are eligible) continue to undergo verification medical exams at a cost to the public pension system (if verification medical exams is required)
- Denied applicants are not advised of their right to appeal
- Deductions for insurance premiums are incorrect or not adjusted when necessary

2. Controls to mitigate the risks

- Require initial medical exams by at least two physicians, one of whom is selected by the public pension system
- Restrict access to medical records only to staff needing access to perform their jobs
- Protect medical information once it has been received by the system
- Promulgate administrative rules to establish timelines for submission of application, employer certification, medical evidence, and other required documentation
- Develop written procedures and checklists to ensure that applications are processed uniformly, completely, and timely
- Require annual signed statements, verifying continued eligibility
- Establish good communication with the Board to ensure proper notification of disability approvals, denials, and revocations

- Establish investigations unit to perform *sub rosa* (secret) investigations to locate documents and witnesses and work with independent medical examiners
- Contract with outside vendor to provide proof of disability ineligibility, if necessary
- Require periodic annual medical evaluations after the disability annuity has been approved (in selected cases warranting periodic reviews)
- Develop statutes which define the earnings limitation for disability annuitants and provide for automatic indexing
- Monitor other income continuously
- Require copies of annual tax returns to verify earnings of disability annuitants
- Match pension records with state tax return data
- Develop an automated edit to identify disability recipients who attain the normal retirement age and no longer need to undergo verification medical exams
- Develop written procedures and standardized letters to inform denied applicants of their right to appeal
- Request medical records which will indicate when disability occurred (before, during, or after state service)
- Approve physicians
- Verify medical licenses on the state medical board's website
- Require certification of physician's qualifications
- Consider hiring a firm to conduct surveillance of annuitants to ensure they are not participating in activities that would be considered outside their capabilities based on their disability.

X. RETIREMENT BENEFITS

A. Defined Benefit Programs (ordinary)

1. Risks

- Annuity is based on incorrect service credit, highest compensation, benefit formula, and/or age
- Payment for unused leave is converted to service credit in error
- Annuity is not recalculated after additional earnings and service are reported
- Annuity is based on named survivor's incorrect date of birth
- Annuity adjustments are incorrect
- Incorrect benefit changes are made for COLA, benefit enhancement, etc.
- Unauthorized changes are made to retirement benefit payrolls within the public pension system, during transport, or at the site where checks/electronic fund transfers are generated
- Deductions for insurance premiums and federal/state tax withholding are not processed correctly or are not adjusted when necessary
- Appropriate annuity adjustments are not made upon death of annuitant/survivor
- Annuity is not terminated timely upon expiration of the guarantee period
- Checks returned to the system are not followed up on
- Annuity payments are made to deceased retirees
- Annuity was terminated in error because of inaccurate report of death
- Suspended annuity is not resumed after contact has been made with lost retiree
- Information reported to federal/state tax authorities is not accurate, causing penalties for the Fund and over/under tax payments for retirees
- Annual tax information is not sent timely to federal/state tax authorities
- Retiree work for a covered employer without being reported, resulting in overpaid benefits
- Military or other allowable service is not correctly determined

2. Controls to mitigate the risks (*see section V, Collection and Maintenance of Member Data*)

- Ensure that correct information is obtained from the member database
- Send a notice of benefits to the annuitant that discloses data used and calculations made in arriving at the amount of the annuity
- Perform deaths matches using SSA Death Master Death File/ updates, state Vital Records, and/or outside vendors
- Require copy of named survivor's SSN and birth evidence at time annuity begins
- Send annual reminders to annuitants to report address changes

- Use SSA's Employee Verification System to identify/correct inaccurate data for named survivor
- Conduct independent account integrity reviews such as comparing amounts and other data changes between years
- Grant access authority to staff only for those programs and specific account information needed to perform their duties
- Require the Security Officer to monitor access security
- Review suspended annuities periodically
- Use addresses that meet U.S. Postal Service addressing standards
- Adjust federal/state tax withholding automatically when annuity amount changes
- Perform edits to assure that all annuities have an expiration date
- Automate processes to eliminate/reduce manual calculations
- Prohibit the same staff person from preparing and verifying the benefit
- Inquire at retirement counseling session whether a person has military service
- Obtain copies of military records

B. Lump Sum Option Plans (LSOP): Forward and Back Deferred Retirement Option Plan Programs (Forward DROP and Back DROP) and Partial Lump Sum Option Plan (PLOP)

1. Risks

- LSOP is not being administered in compliance with state law, rule, or regulation
- LSOP account is improperly maintained
- Correct tax withholding is not taken if LSOP account is withdrawn and not rolled over to a qualified plan/IRA
- Participants are still contributing/earning service credit while in LSOP
- Contributions are not resumed when LSOP ends and employee continues to work
- LSOP is not accounted for properly in the audited financial statements

2. Controls to mitigate the risks

- Create a charter that includes the objectives and responsibilities of the LSOP program
- Develop procedures for the creation, maintenance, and termination of LSOP accounts
- Provide continuing training to employees working in the LSOP program
- Provide proper internal controls and adequate accounting for the LSOP program
- Provide proper financial accounting for LSOP programs. Determine whether LSOP program transfers defined benefit payments into a defined contribution plan, so that LSOP is a defined contribution plan for financial accounting and reporting purposes

XI. DEATHS/SURVIVOR BENEFITS

1. Risks

- Death of retiree is not received/recorded promptly, resulting in overpayments
- Benefits are not stopped as soon as death is confirmed
- Deaths of annuitants living outside the U.S. are not identified
- Death is not identified because system has incorrect SSN
- Living person is reported as deceased, thus terminating annuity in error
- Independent sources or documents are not used to verify accuracy of death data
- Death benefits are issued prior to the return of outstanding overpayments
- Annuity overpayments are not identified, recorded, and collected
- Decedent account has accumulated significant over/underpayments
- Some or all beneficiaries cannot be located
- Annuity is not reduced/adjusted, if applicable, when continuing to beneficiary
- Benefits are paid to surviving spouse, ex-spouse, other beneficiaries, or estate not entitled to the benefits
- Unclaimed benefits are paid out to unauthorized individuals
- Survivor benefits are paid to persons no longer eligible or after the annuity expiration date
- Benefit is not divided correctly between spouse and children
- Benefits to minors are not monitored/terminated upon their reaching the age of majority
- The Fund does not verify if students are enrolled in school full-time, if required
- The Fund does not comply with IRS minimum distribution requirements to beneficiaries
- Incorrect death benefit is paid (active vs. inactive) to survivor
- As deaths are entered into the system, they are not reviewed by another person to verify that data was entered correctly
- Deaths reported by outside contractors are not followed-up on in a timely manner
- Procedures are not in effect to adequately obtain information on the deaths of retirees, beneficiaries and survivors on a timely basis
- The Fund does not require proof of eligibility from survivors

2. Controls to mitigate the risks

- Perform death matches with SSA and state vital records
- Hire outside vendors to conduct death matches
- Search Internet periodically for online death notices
- Use newspaper/ periodical clipping service in area, if available, to identify deaths

- Send annual reminders (statements, newsletters, correspondence) to members and beneficiaries, requesting they report address changes, and beneficiary changes
- Identify annuitants living outside the U.S. with a special code on the annuity system and send annual confirmation letters to them, stop benefits if signed confirmation letters aren't returned
- Use SSA's Employee Verification System to identify incorrect SSNs
- Require death certificates for member files
- Verify SSA reported deaths before terminating annuities (include telephone calls, certified letters, and other means)
- Verify eligibility for continued payments by annual certification forms signed by spouses and children
- Compile a list of beneficiaries who do not receive benefits when first eligible and send annual letters to them
- Carefully validate the employment history to identify dates of service that are consistent with death benefit payment type
- Ensure that verification of survivor benefit eligibility and benefit calculation occurs prior to initial payment being issued
- Annually verify eligibility of survivor benefits for individuals where the benefit is not payable until death to ensure eligibility criteria is still met (e.g., student survivor)
- Perform in person verification of retirees over a certain age and/or living in a foreign country to confirm continued eligibility of benefits

XII. SERVICE CREDIT PURCHASES / PORTABILITY / RECIPROCITY / TRANSFERS

1. Risks

- Portability/reciprocity data is not received and/or entered properly
- Purchase of prior service is incorrectly allowed or incorrectly rejected
- Prior service credit is incorrectly calculated
- Cost of, and payments for, prior service credit are incorrectly calculated
- Prior service credit is incorrectly recorded in the system
- A member's service credit balance is inappropriately adjusted or altered
- Retirement plan contribution transfers are accepted from non-qualified plans
- Receivables for buy-backs/transfers are not properly established
- Checks/payments for buy-backs/rollovers are not properly safeguarded, transferred, cashed, and credited to the correct member account

2. Controls to mitigate the risks

- Develop quality assurance reviews to ensure service credit is properly posted to the member's account
- Configure computer system according to plan statute regarding service credit purchases to ensure transactions are accepted and rejected accordingly
- Review factors used in the actuarial calculation for service purchases and transfers before being provided to the actuary for calculation

XIII. ACTUARY

A. Assumptions

1. Risks

- Actuarial assumptions are not realistic or based on outdated facts
- Actuarial assumptions are made on erroneous/inaccurate data
- Political pressure is exerted to modify assumptions that do not reflect reality
- Mortality tables are not updated as appropriate

2. Controls to mitigate the risks

- Discuss actuarial assumptions at Board meetings prior to making any changes to the demographic or economic assumptions
- Require that knowledgeable staff review actuarial report
- Have an actuarial valuation prepared at least biennially by a qualified actuary in accordance with the principles and procedures established by the Actuarial Standards Board (ASB), based on a discussion with the actuary of funding methods and assumptions (GFOA recommended practice)
- Hire an independent actuarial firm at least every five years to audit actuarial assumptions
- Perform a year to year comparison of the number of participants in each classification group (i.e., active, inactive, retired) and evaluate key trends or changes
- Update mortality tables periodically (for example, every 5 years)
- Have the actuarial valuation process reviewed by several independent parties, including an oversight committee to determine if assumptions are correct

B. Assets/Liabilities

1. Risks

- Actuarial assets and liabilities are not matched (asset-liability study)
- Assets of the public pension system do not support liabilities because actuarial assumptions of future investment returns prove to be inaccurate, actuarial assumptions of liabilities are different than actual experience, or legislative actions result in benefit and funding levels that are not supported by sufficient contributions or assets based on actual market returns

2. Controls to mitigate the risks

- Establish a period for amortization of unfunded actuarial accrued liabilities that conforms with the parameters established by Governmental Accounting Standards Board (GASB) (GFOA recommended practice)
- Ensure that actuarially required contributions are collected timely and not postponed or reduced (GFOA recommended practice)
- Have an actuarial experience study performed at least once every five years (GFOA recommended practice)
- Assign in-house staff with actuarial knowledge to review work of outside actuary
- Hire an independent actuarial firm preferably every two years, or at a minimum of once every five years, to perform an audit of the actuarial valuations (GFOA recommended practice is at least once every 10 years)
- Implement entry/exit analysis to review trends and data changes from year to year
- Have a periodic actuarial audits and reviews of contribution levels to ensure integrity of funding methods and processes
- Consider hiring an in-house actuarial specialist

C. Actuarial Computer Program (Algorithm)

1. Risks

- Actuarial computer program (algorithm) is incorrect
- Actuarial models have not been properly updated to reflect changes in benefit formulas
- Actuarial models do not conform to, or are not updated for, applicable laws, and/or changes in the laws
- Actuarial reduction factors for those retiring before normal retirement age are not accurate
- Programming does not correctly analyze data
- Changes made to the actuarial computer program not adequately tested prior to being put into production causing errors

2. Controls to mitigate the risks

- Hire an independent actuarial firm at a minimum of once every five years to perform audit of the actuarial valuation that includes a parallel calculation of actuarial liabilities
- Develop a quality assurance program for Information Technology (IT) and operations staff to validate that the data was correct and analyses accurate
- Thoroughly test actuarial data file before releasing to the system actuary

D. Data

1. Risks

- Data transmitted to the actuary is incomplete/erroneous
- Contribution data used is based upon payroll data rather than cash received
- Data exceptions or errors noted by the actuary are not researched/corrected timely
- Programming does not correctly analyze data
- Errors, noted by the actuary in data sent to them, are not corrected on the computer system

2. Controls to mitigate the risks

- Develop reasonableness checks that identify possible data errors
- Conduct data audits
- Develop controls to determine reliability of data received, data input, and data maintenance
- Require that contributions are based solely upon cash received
- Require that exceptions and errors be researched and corrected timely
- Use computer assisted audit techniques to evaluate data and identify change anomalies from year to year
- Develop quality assurance of programming by IT and operations staff to validate data was correct and analyses accurate
- Implement entry/exit analysis to review trends and data changes from year to year
- Thoroughly test the actuarial data file before releasing to the system actuary
- Forward to appropriate public pension system's staff data errors found during testing so that correction can be made timely

E. Employer Contribution Rates

1. Risks

- Employer contribution rates are not accurate due to program or data errors
- Employer contribution rates are not sufficient to fund benefits

2. Controls to mitigate the risks

- Require annual presentations by the actuary to the Board, including discussions of employer contribution rates and specific changes to rates
- Hire an independent actuarial firm at a minimum of once every five years to perform audit of the actuarial valuation that includes a parallel calculation of contribution rates

- Compare analysis of the valuation of future liabilities to contributions and return on investments to determine if benefits are properly funded
- Consider hiring consultants to communicate the importance of adequately funding the plan in accordance with actuarially suggested employer and employee contribution rates

F. Employer Contract Changes – Cost of Providing Estimate of Potential Changes to the Benefit Structure

1. Risks

- Employers/employee groups are overcharged or undercharged for the cost to produce an estimate of the effects of changing benefits or other employer contract provisions, resulting in a monetary subsidy or loss to the groups using the service
- Employers/employee groups are undercharged for the cost to produce an estimate of the effects of changing employer contract provisions, resulting in numerous requests to the actuaries so that excessive resources are diverted to these services

2. Control to mitigate the risks

- Develop a cost accounting data system to determine the cost of estimates and charge employers these amounts

XIV. COMMUNICATION WITH EMPLOYERS

A. Employer Responsibilities

1. Risks

- Employer staff are not adequately trained for their responsibilities
- An agency is not correctly submitting required information, payrolls, contributions to the Fund

2. Controls to mitigate the risks

- Provide training for new staff responsible for reporting, etc.
- Perform quality assurance reviews of data/information and random audit of selected data/information
- Develop and provide Employer Manual that includes periodic updates that are clear and accurate
- Educate employer agencies on the procedures regarding submitting required documents
- Ensure system edits are in place to prompt staff when required documents need to be requested from the agency
- Use checklists or procedures to ensure required documents are sent
- Conduct employer audits

B. Member Services

1. Risks

- Employer benefit specialists are not given adequate information and training to communicate pension plan provisions to employers
- Inadequate information is transmitted to the employers on benefit plans and services available (i.e., brochures, Internet access, telephone services, and walk-in opportunities)

2. Controls to mitigate the risks

- See *section VI*, *Communications with Members*
- Provide information and ongoing training to all employer benefit specialists
- Provide high quality brochures, internet information, telephone service, and customer service representatives

C. Contribution Rates

1. Risks

- Employers are not given adequate notice of anticipated changes in employer contribution rates, and reasonable estimates of the magnitude of changes
- Public pension system staff does not notify employers timely of changes in employee and employer contribution rates once the new rates are calculated
- Employers are not given adequate reasons for changes in employer contribution rates
- Employer does not update programs for contribution rate changes, resulting in inaccurate contributions
- Communication errors between investment staff and other public pension system staff regarding earnings or losses, resulting in public pension system staff providing incorrect rates to employers

2. Controls to mitigate the risks

- Perform evaluations and inform the employer promptly of changes in employer contribution rates; provide explanation of the changes
- Input data from employers into contributions accounting system(s) timely
- Validate contributions independently to ensure rates are accurate
- Match contribution rates paid with contribution rates required by the actuary
- Perform supervisory reviews and reasonableness checks to identify obvious errors in actuarial assumptions including investment earnings/losses and in contribution rate calculations
- Perform employer payroll audits

XV. CONTRACTING WITH SUPPLIERS OF GOODS AND SERVICES

A. Operations Contracts (Ordinary)

1. Risks

- Object of contract is not adequately defined
- Contract terms are not complete or adequate for the project/tasks required
- Bid procedures are not properly followed
- Contracting process is difficult to comply with, increasing the potential for noncompliance and making it difficult for business units to meet their objectives
- Consultants are working on contracts not related to the Fund while utilizing the Funds' facilities, equipment and supplies
- Adequate due diligence is not performed for major suppliers before hiring
- Financial status of major suppliers is not monitored through review of audited financial statements, popular press articles, and internet searches
- Contractor does not complete adequate background history check for all hires who work on the contract
- Contract employees engaged in inappropriate activities before hire and/or during employment, including criminal activity, unethical conduct, and fraudulent activity
- Noncompliance with a contract provision occurs
- Payments made to contractor are not in accordance with contract terms

2. Controls to mitigate the risks

- Require the legal counsel to review contracts
- Ensure both parties have a mutual understanding of the terms of the contract
- Provide a sample of the contract up front (in the RFP) when negotiating a deal with the vendors, or provide a sample contract at the start of the negotiations
- Ensure that all relevant public pension system staff have reviewed the Request for Proposal (RFP) and/or proposed contract
- Do an Internet search of applicant's possible involvement in lawsuits, settlements, fraud, and kickbacks
- Request detailed description of hiring practices and procedures from the vendor
- Include in the contract the ability of the public pension system to do independent background checks (i.e., require SSN/INS # and date of birth for all contract employees)
- Include a mandatory clause in the contract that clearly states that the public pension funds' facilities and supplies are to be used only for the public pension

funds' related projects. Also, require that while on the property, only public pension system projects are to be worked on. Require the contract manager to monitor what the consultant is doing while on the premises

- Ensure that a signed contract is in place before outsourced services or products are procured. Ensure background checks are performed on contract personnel
- Establish process to review compliance with contract terms

B. Third-Party Administrator (TPA) Contracts

1. Risks

- Adequate due diligence is not performed on TPA applicants
- Contract employees engaged in inappropriate activities before hire and/or during employment, including criminal activity, unethical conduct, and fraudulent activity
- Contract provisions are inadequate
- TPA does not understand its fiduciary duty
- Public pension system management does not appropriately monitor the TPA
- An annual Statement on Standards for Attestation Engagements (SSAE) No. 16, Type II (formerly SAS 70) audit is not performed by the TPA's independent auditor, not transmitted to the public pension system and not reviewed by the public pension system staff
- TPA's audited financial statements are not received/reviewed by public pension system staff
- Contract does not contain an audit clause
- TPA has a conflict of interest
- TPA destroys records that should be maintained
- The plan is not administered in accordance with contractual agreement
- Communication lines between third party and the public pension system are not clear causing a misunderstanding of expectations
- Sensitive data is not handled in a secure manner by third parties

2. Controls to mitigate the risks

- Develop policies and procedures for performing due diligence
- Do Internet search of applicant's possible involvement in lawsuits, settlements, fraud, and kickbacks
- Require a clause in the contract with the vendor for background checks, including evidence to show that detailed background checks have been conducted

- Obtain copies of SSNs for contract employees, thus permitting the public pension system to conduct its own background checks and run edits on SSNs
- Develop standard contract provisions
- Include fiduciary duties terms in the contract
- Require that contract managers have training in monitoring compliance
- Require a SSAE 16, Service Organization Control (SOC) 1), Type II, report in the RFP and in the contract. Depending on the service external parties provide, the public pension system may instead need SOC 2, Type II, or SOC 3.
- Require that contractor forward its audited financial statements to the appropriate staff of the public pension system
- Require sign-off by the appropriate staff of the public pension system that they have reviewed the financial statements
- Require standard contract language in RFPs and contracts
- Require the legal counsel to review TPA contracts
- Require TPA to complete financial disclosure/conflict of interest certification annually
- Include a contract clause giving the public pension system the right and ability to do independent background checks (i.e., require SSN/INS # and date of birth for all contract employees)
- Include a contract clause that identifies the owner of the records
- Include a contract clause on records retention schedule
- Include contract provision requiring the proper safeguard and destruction of sensitive data

XVI. BUSINESS CONTINUITY PLANNING

1. Risks

- There is no business continuity plan
- The business continuity plan does not facilitate timely resumption and performance of duties after a disaster
- The business continuity plan does not adequately address important issues such as utility supply, travel requirements, hot site location, etc.
- The business continuity plan is not regularly tested, periodically reviewed, and updated
- Business continuity plan is not properly communicated to staff
- Staff are not aware of the business continuity plan or how to properly execute it
- External service providers do not have business continuity plans

2. Controls to mitigate the risks

- Assign a specific staff responsibility for the business continuity plan
- Create a risk-based business continuity plan with cooperation from business units. Require business units to identify critical processes and assign priorities so that systems are operational within a specified time frame after an emergency or business continuity event. Include essential issues in the business continuity plan such as resuming IT access off-site, resuming phone and LAN based services, serving participants face to face, purchasing and obtaining equipment, providing mail services, relocating users, etc.
- Develop checklists and/or written procedures for business continuity, including expected results; review/update these periodically
- Develop a schedule for reviewing and maintaining the business continuity plan, including a reasonable budget for testing and maintaining key components (such as disaster recovery of information technology components) to ensure the items/equipment/data exist, are useful, and could replace live operations
- Develop a plan for ongoing communication of information relating to the business continuity plan
- Discuss business continuity plans with external service providers and determine how they will continue business in the event of a disaster that affects their business

XVII. CASH FORECASTING

Note: This section is limited to activities related to cash forecasting for a separate benefits entity or division. Cash forecasts should be an integral part of a comprehensive cash management system that is generally run by the accounting and investment divisions of a public pension fund or by a separate government investment agency. Risks of a comprehensive cash management system would be best addressed in a document on investment risks.

1. Risks

- There are no comprehensive policies and procedures for cash forecasting
- There is no coordination between cash forecasting with the cash management program of the accounting or investment division/agency
- There is no accurate forecast of the sources and uses of cash
- Sources and uses of cash are not included in the forecast
- Cash is not available to pay benefits and operational expenses
- Cash forecasts are not updated to reflect benefit structure changes
- Investment returns are not maximized due to poor cash forecasting

2. Controls to mitigate the risks

- Assign a cash flow manager
- Develop comprehensive written policies and procedures for cash forecasting including the required coordination between accounting and investment divisions/agency
- Create a comprehensive listing of disbursements for benefits (retirement, disability, or death), refunds, and operational expenses. Create a comprehensive listing of various cash receipts such as employer contributions, member contributions, and service purchases
- Hire staff who are knowledgeable in cash forecasting
- Perform an asset/liability study (*see section XIII, Actuary*)
- Prepare and document cash forecasts at least two years into the future
- Compare and document actual cash flows with the cash forecast monthly; adjust remaining cash forecasts and the cash forecasting process as appropriate
- Monitor employment cycles, external events, and governing body actions which may affect cash flows

XVIII. ACCOUNTING

A. Managerial Accounting and Reporting

1. Risks

- Pension plan is costly and inefficiently run because various processes are inefficient, ineffective or not needed. Costs of various processes are not calculated
- Costs relevant to various processes are grouped and inappropriately hidden in general classifications such as overhead and administration
- Public pension system does not have an activity-based cost accounting system that tracks the costs of various processes
- Public pension system does not have staff that are knowledgeable and current in cost/managerial accounting and GASB requirements

2. Controls to mitigate the risks

- Create a charter that includes the objectives of cost/managerial accounting
- Perform costing studies of existing processes and reengineer as appropriate
- Perform costing studies as new processes are created
- Hire staff who are knowledgeable and current in cost/managerial accounting
- Encourage existing staff to obtain training in and certifications in cost/managerial accounting. The most relevant certifications are the Certified Management Accountant (CMA), Certified Financial Manager (CFM), Certified Government Auditing Professional (CGAP), and Certified Public Accountant (CPA)
- Implement an activity-based costing system
- Send periodic internal financial reports to an independent Board/Audit Committee

B. Financial Accounting and Reporting

1. Risks

- Financial statements, both interim and year-end, do not provide useful information for the various groups of users
- Financial information is not relevant and reliable
- Financial statements do not fully disclose all material items
- Financial statements do not disclose sufficient detail (statements, footnotes, and required supplementary information) to permit analyses and understanding of each area
- Financial statements are not organized and formatted to permit analyses and understanding

- Financial statements have material errors and/or irregularities
- Financial statements do not conform to generally accepted accounting principles (GAAP/GASB)
- Financial statements are not fully informative because they present only the minimum disclosures required by GAAP/GASB
- Management's Discussion and Analysis does not explain the reasons behind the numbers and the changes in these numbers from prior periods (i.e., transparency)
- Financial statements are not provided in a timely manner for auditing
- Adequate controls may not be in place for maintaining and monitoring general ledger accounts
- General ledger accounts are not reconciled timely and accurately
- Journal entries are not recorded or classified in accordance with applicable accounting standards
- Management does not review and approve the financial reports that are produced

2. Controls to mitigate the risks

- Create a charter that includes the objectives of financial reporting, including both interim and year-end financial statements, and ad hoc reports
- Hire staff with relevant training and professional certifications and encourage and facilitate existing staff in obtaining training and professional certifications. Appropriate certifications include the CPA, CMA, CFM, Chartered Financial Analyst (CFA), CGAP, and Certified Government Financial Manager (CGFM)
- Pay for professional exams, professional meetings, continuing professional education, and annual certification maintenance fees
- Encourage accounting staff to participate in professional societies and sit on boards of these societies
- Provide continuing education for staff involved with preparation of financial statements
- Hire reputable independent, external CPA firm knowledgeable of public pension plans
- Compare reporting to applicable standards (e.g., GASB, American Institute of CPAs (AICPA), etc.) and other public pension system reports
- Compare reports to other reports receiving the GFOA Certificate of Achievement for Excellence in Financial Reporting
- Hire temporary employees to assist in the timely preparation of year-end statements
- Perform interim closings (for example, quarterly) to improve the timeliness and efficiency of year-end closings

- Consider rotating external auditors on a periodic basis
- Perform and approve general ledger account reconciliations regularly
- Have all journal entries documented, reviewed, and approved by financial management prior to posting
- Present financial statements to members of the Audit Committee, if applicable, for review

C. Cash Receipts

1. Risks

- There are no comprehensive policies and procedures for receiving and depositing cash, checks, and electronic forms of payment
- There is inadequate separation of duties for receiving and recording cash receipts
- A payment received is for the incorrect amount
- Payments are not deposited the same day as received
- Investment division/agency is not notified of cash deposits
- Cash may be embezzled
- Affected general ledger accounts are not reconciled regularly

2. Controls to mitigate the risks

- Create comprehensive written policies and procedures for receiving/depositing cash
- Create adequate separation of duties for handling cash receipts and cash accounting
- Use a bank lock box for receiving cash and checks
- Reconcile cash receipts to the appropriate source documents to ensure that the correct payment amount has been received
- Track deposits to determine if 100% of receipts are deposited same day
- Reconcile cash received to cash deposited to ensure all receipts are deposited intact and not misappropriated
- Require employees to take annual vacation.
- Notify the investment division/agency of deposits received, if necessary
- Perform periodic account reconciliation

D. Accounts Receivable

1. Risks

- Checks are not logged in as they are received
- Receivables are not invoiced
- Receivables are invoiced, but are not recorded or improperly recorded

- Lapping of accounts receivable payments
- There is no method or an inappropriate method is used to determine and monitor the allowance for doubtful accounts
- Accounts receivables are written off without authorization
- Affected general ledger accounts are not reconciled on a routine basis

2. Controls to mitigate the risks

- Maintain a log to record receipt of checks
- Segregate duties within the accounts receivable function
- Use of system generated, pre-numbered invoices
- Require all employees to take annual vacation
- Age accounts receivable appropriately based on history and industry standards
- Review accounts receivable aging regularly
- Establish and adhere to write-off policies and procedures
- Require that only authorized personnel may write off receivables
- Perform periodic account reconciliation

E. Accounts Payable

1. Risks

- Payments are made that are inappropriate, unauthorized, or lacking adequate supporting documentation (including duplicate payments)
- Vendor invoices are not paid timely
- Vendor discounts are not taken advantage of
- Payments are made to an unauthorized vendor
- Modifications are made to master vendor list without prior approval
- Affected general ledger accounts are not reconciled on a routine basis

2. Controls to mitigate the risks

- Review payment requests for appropriate authorization and supporting documentation prior to payment processing. A list of authorized signors should be maintained
- Require adequate supporting documentation prior to issuing payment
- Require independent review of payments prior to issuance
- Cancel invoices upon payment
- Ensure that the accounting system restricts duplicate invoices and duplicate payments to the same invoice
- Ensure that discounted payment terms are identified within the system and are taken based on policy

- Have the master vendor list modifications approved by an appropriate level of management
- Ensure that vendor master file update capabilities are restricted to appropriate users
- Perform periodic account reconciliation

F. Employee Payroll

1. Risks

- Employees are paid the incorrect amount
- Unauthorized payments are made to employees
- Payments are made to fictitious employees
- Payments to retirement, insurance, IRS, and other outside vendors are inaccurate and/or untimely
- Reporting to the IRS, SSA, employees (W-2), and other outside vendors are inaccurate and/or untimely
- Time reports are falsified or not properly approved
- Leave accruals are not applied properly to eligible employees or at the incorrect rate
- Non-compliance with payroll laws (fair labor standards, IRS, etc.)
- Affected general ledger accounts are not reconciled on a routine basis

2. Controls to mitigate the risks

- Review all payroll changes for proper authorization and accuracy
- Generate and review payroll exception report to identify anomalies in employee pay from one pay period to the next
- Perform periodic payroll audit
- Ensure a proper segregation of duties between the human resource and payroll function
- Develop a process to ensure payments for all withholdings and deductions are accurate and made timely
- Develop a process to ensure payroll reports to external parties and employees are accurate and issued timely
- Ensure that time reports are reviewed and approved by supervisor and payroll clerk prior to payment
- Configure computer system to only allow leave accrual for employees types that are eligible
- Review leave accrual rate changes as part of payroll cycle
- Perform periodic account reconciliation

G. Purchasing

1. Risks

- Purchases may be received but never reported, or reported inaccurately
- Purchases may be stolen, destroyed, or intentionally diverted
- Purchases are not properly approved
- Employees with purchasing authority have a perceived or actual conflict of interest
- Fraud can occur in various forms such as ghost vendors, kickbacks, purchase of personal items, deliveries to employee homes, etc.
- Bidding procedures are inadequate or not complied with
- Purchasing cards (p-cards) are misused or issued to inappropriate personnel
- Affected general ledger accounts are not reconciled on a routine basis

2. Controls to mitigate the risks

- Review the vendor's invoice or equivalent for authorization, receipt of material or services, and accuracy of price and quantity. The absence of any of the referenced information or discrepancies between the information must be resolved before payment is made
- Analyze purchasing transaction records for unusual items, frequent purchases, items of high value
- Perform periodic inventory audit on items of value and/or appeal
- Spot check purchased items for verification of possession
- Require all employees to take annual vacation
- Rotate employees in areas with high risk of fraud
- Segregate the accounts payable function from purchasing and receiving activities from general ledger recording activities
- Ensure bidding procedures are adequate and complied with
- Review p-card transactions
- Issue p-cards only to authorized personnel
- Perform periodic account reconciliation

XIX. EXTERNAL AUDIT

1. Risks

- External audit firm is not independent
- External audit firm personnel have a conflict of interest
- External audit firm does not have sufficient knowledge of public pension system in order to perform a proper audit (deficient knowledge of the industry)
- External audit firm's personnel (engagement partner, manager and on-site supervisor) assigned to the audit do not have sufficient experience and knowledge of the public pension system
- External audit firm does not have access to appropriate actuarial staff to evaluate actuarial information
- External audit firm is not registered in the state where audit occurs
- External audit firm key personnel (engagement partner, manager, and on-site supervisor) assigned to the audit do not have the CPA license
- External auditors fail to identify material misstatements or omissions in the financial statements
- External auditors do not identify financial statements that are not in accordance with GAAP
- External auditors do not identify material weaknesses in internal controls
- External auditors do not perform enough work to support their conclusion/opinion (may result from low-balling when bidding the contract)

2. Controls to mitigate the risks

- Hire a reputable independent, external audit firm knowledgeable of public pension plans
- Identify all of the services the external audit firm is performing for your public pension system, and determine if there is a conflict of interest
- Limit the external audit firm's services to performing audit and attest services only
- Require periodic mandatory rotation of audit partners or perhaps of external audit firms
- Evaluate periodically the independence of the external audit firm and its key personnel
- Require the Board or Audit Committee to approve all services rendered by the external audit firm, in addition to the annual financial statements audit
- Review the qualifications of the external audit firm, engagement partner, audit manager, and on-site supervisor. A good minimum qualification is a CPA

certificate for all key personnel, and experience in auditing public pension funds. All key personnel and changes in key personnel should be pre-approved in writing by the Audit Committee or Chief Audit Executive.

- Monitor external audit firm work during engagement. Require a weekly status meetings
- Interact with/discuss issues with key personnel of the external audit firm (i.e., Partner, Manager, on-site supervisor)
- Follow-up periodically with the public pension system's accounting manager to determine external audit firm progress, work quality, level of understanding, customer service, etc.
- Perform review of external audit firm's work papers (by Internal Audit), if allowed
- Require that external auditors complete financial disclosure/conflict of interest statement annually
- Require that external auditors do not perform any non-audit services which go beyond the Sarbanes-Oxley Act and SAS requirements
- Review the Sarbanes-Oxley Act to determine if there are items which your public pension system wishes to adopt voluntarily
- Develop a written policy on the responsibilities of external auditors

XX. INTERNAL AUDIT

1. Risks

- There is no internal audit function
- The internal audit function is not organizationally independent of operations (improper reporting structure)
- The chief audit executive does not report to a level within the organization that allows the internal audit activity to fulfill its responsibilities
- Internal audit plan is not risk-based, inadequate, and/or not updated
- Internal audits are not performed in accordance with the International Standards for the Professional Practice of Internal Auditing published by The Institute of Internal Auditors (The IIA Standards)
- Internal audit work papers are not retained for a sufficient period of time
- Internal auditors do not have an effective working relationship with the Board and/or Audit Committee
- Internal auditors have a strained relationship with public pension system management and staff and do not communicate adequately with auditees in order to obtain their support for corrective risk mitigation strategies
- Internal audit function is not, or is not perceived as, adding value to system
- Internal audit management and/or staff do not have sufficient expertise/training in auditing public pension funds
- Internal audit staff are not encouraged to obtain appropriate profession certifications, such as the Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), CPA, Certified Fraud Examiner (CFE), Certified Investments and Derivatives Auditor (CIDA), CGFM, CMA, CGAP, CFM or other relevant certifications
- Internal audit staff are not encouraged to participate in relevant professional societies and to obtain continuing professional education

2. Controls to mitigate the risks

- Create an internal audit function with appropriate and adequate resources (experienced audit personnel, adequate budget, etc.)
- Require that internal audit has a charter approved by the Board and/or Audit Committee
- Require that the Chief Audit Executive report to a level within the organization that allows the internal audit fulfill its responsibilities
- Require the Chief Audit Executive to confirm to the Board, at least annually, the organizational independence of the internal audit activity.

- Develop internal audit policies and procedures manual and obtain Board or Audit Committee approval
- Maintain audit records for at least seven years or as required by state law
- Develop an internal audit record retention policy
- Conduct an external assessment of the internal audit function at least once every five years by a qualified, independent assessor or assessment team from outside the organization in accordance with the requirements of The IIA standards.
- Develop internal quality assessment process to ensure compliance with The IIA standards and internal audit policies and procedures. There should be ongoing quality assurance procedures and periodic internal self-assessments to ensure compliance with The IIA standards
- Develop an audit scope that is sufficient, refined, and limited so as to accomplish audit objectives in a reasonable time frame
- Consider sending customer satisfaction survey to auditee at end of each audit or assignment
- Require the Chief Audit Executive to meet with the Board, Audit Committee, and management periodically
- Require that internal auditors obtain adequate training in auditing and public pension funds on a regular basis
- Encourage internal auditors to obtain relevant professional certifications, such as the CIA, CISA, CPA, CMA, CFM, CFA, CIDA, CGAP, CFE, CGFM, etc.
- Encourage internal auditors to participate in professional organizations and sit on the boards of these organizations
- Pay for professional examination fees, professional meeting costs, continuing professional education, and annual certification maintenance fees

XXI. CONSULTANTS

1. Risks

- Contract manager does not have sufficient experience and expertise to manage the consultant contract appropriately
- Contract manager does not hold consultants accountable for contracted deliverables
- Designated contract manager is not the appropriate person to manage the consultant contract (examples: Project Manager managing the oversight consultant's contract; consultant managing another consultant's contract)
- Consultant does not have adequate skills or expertise in the area of hire
- Consultant is not eligible to work in the United States
- Consultant hiring practices do not include a thorough background check of both resident and non-resident foreign staff
- No one has responsibility for performing background checks of information systems consultants to determine that they have appropriate backgrounds to have access to key systems (for example, pension system staff assume in error that the consultant company performs background checks but it does not)
- Consultant has employees who engaged in inappropriate activities before hire and/or during employment, including criminal activity, unethical conduct, and fraudulent activity
- Consultant has a conflict of interest
- Consultant is hired because of political connections
- Consultant does not understand the organization
- Consultant does not understand the fiduciary responsibility to members, retirees, and beneficiaries
- Payments to consultant are not tied to deliverables
- Consultant does not transfer knowledge to public pension system staff or that staff do not acquire knowledge from the consultant, resulting in consultant's continued presence
- The public pension system hires consultants to perform work that could be done by competent public pension system staff
- Contract with consultant does not include all provisions to ensure that the consultant is an independent contractor under applicable laws and U.S. Department of Labor definitions

2. Controls to mitigate the risks

- Ensure internal staff have sufficient experience, technical knowledge of the subject of the contract, and expertise to manage consultant contracts
- Monitor contract management activities to ensure contract manager is adequately managing the contract, i.e., holding consultant accountable for deliverables and measuring deliverables against quality standards
- Identify required minimum levels of experience and expertise and ensure that consultant meets the minimum requirements
- Require a contract clause for detailed background checks, including submission of adequate evidence to prove that required background checks was conducted
- Confirm that consultants are eligible to work in the United States
- Use the Terrorist Database issued by the U.S. Treasury or public databases for convicts to ensure that consultants meet background criteria
- Establish a process, including assignment of responsibility, to determine that information systems consultants have appropriate backgrounds to have access to key systems
- Review resumes to determine if consultants have the required skills and experience
- Obtain copies of SSNs for employees of the consultant, thus permitting the public pension system to conduct its own background checks
- Provide the consultant with an orientation to the organization
- Implement contracting standards and a uniform process
- Establish an independent contracting and RFP office
- Ensure that deliverables and deadlines are spelled out in the contract and are tied to payments. Include penalties for not meeting deadlines and submitting deliverables timely
- Require Board approval for contracts that exceed a certain dollar amount
- Require that consultants complete financial disclosure/conflict of interest statement annually
- Review invoices for appropriateness of charges
- Ensure that contracts, requirements, and working conditions of the consultant meet the U.S. Department of Labor definition of a consultant

XXII. INFORMATION TECHNOLOGY

A. Information Systems Acquisition and Development

1. Risks

- Project goals do not support the mission and strategic plan of the pension system
- Pension plan does not have information systems policy that includes the entire system development life cycle (SDLC)
- SDLC does not have a formal quality assurance process or the formal process is not effective
- Project implementation does not follow a body of standards
- The process for system acquisition or development is not monitored by an individual or oversight committee
- Projects are not formally approved prior to initiation and resource allocation
- Project is not adequately scoped, defined, and justified
- Systems development life cycle process is inadequately managed
- Pension plan staff/manager does not have the technical expertise to effectively manage the project
- Project does not have adequate support from the Board, Executive, Department, or user groups
- A formal project management process is not used or not deployed effectively. Formal project management includes project methodology and plans, project tools, realistic project milestones, and project deliverables that enable project manager to efficiently manage, control, and direct the project. Project management also includes management of risk, issues, and scope changes; a criticality assessment of the project; and management and oversight appropriate to the criticality level.
- Formal development standards are not followed
- Project roles and responsibilities are not clearly defined
- Project tools are not used in a consistent manner
- Project deliverables are not consistently developed
- Payments are not tied to deliverables
- Test plans and test data are not adequate
- System and/or user acceptance testing is not performed or not adequately performed
- The testing period is shortened to meet deadlines
- Volume and stress testing is not performed or not adequately performed
- System acceptance criteria is not identified, documented, evaluated, or approved

- Appropriate personnel are not consulted throughout the project, such as those responsible for disaster recovery, security, and telecommunications
- Security and audit functions are not built into the system and configured properly
- User requirements or business objectives are not met
- Interfaces with other internal and external systems may not function properly
- Data in the old system is not properly converted to its correct value in the new system
- Adequate resources are not available to maintain the system
- Ongoing maintenance costs have not been included in cost-benefit analysis or that management does not fully realize future costs to maintain the system
- Adequate and appropriate system documentation is not available at the conclusion of implementation
- Staff not be trained adequately in order to operate the system correctly

2. Controls to mitigate the risks

- Implement a SDLC policy
- Develop a formal information technology (IT) quality assurance process as part of SDLC
- Create guidelines for project initiation, objectives, success criteria, scope, justification, and approval
- Follow a body of standards such as the Institute of Electrical and Electronics Engineers (IEEE), Control Objectives for Information Technology (COBIT), or Project Management Institute (PMI)
- Ensure that test plans are thorough, complete, and reliable (developed by operations staff along with user groups)
- Ensure that system is tested by both functional and technical staff
- Require that all project managers have adequate managerial/technical expertise
- Encourage IT staff to become certified in relevant areas
- Require a formal project management process that follows the chosen standards for all projects
- Require that payments are tied to project deliverables
- Develop a quality standard against which deliverables are measured
- Provide milestone reports to oversight committees and management
- Involve personnel from all affected units
- Require the involvement of internal auditors during the project so that system controls and any changes to system controls are evaluated timely
- Test and approve security configuration

- Develop and maintain a user security role matrix which outlines the access each role has to each aspect of the system
- Ensure audit trails and security functions in line with the public pension system's security practices are included in the system
- Provide training in project management, systems development and implementation, quality practices, and standards
- Evaluate the need for system volume and stress testing
- Perform management oversight reviews to ensure that system development projects comply with applicable standards, regulations, controls, and management practices
- Consider active user participation and sign-off on project activities such as requirements, specifications, design approaches, test plans, controls procedures, and file conversion results
- Develop system acceptance criteria
- Ensure that system and user acceptance testing is performed as planned
- Ensure that robust reconciliation processes are in place to verify that the data conversion process is properly executed
- Include ongoing maintenance costs in the cost-benefit analysis and discuss with management
- Ensure that adequate, skilled resources are available to maintain the system
- Ensure system documentation is reviewed and available at the conclusion of the project. This documentation should include the technical and functional aspects of the system
- Complete and review procedural updates prior to project implementation
- Develop and adhere to a training plan that extends several months beyond the project implementation

B. Information Security

1. Risks

- Public pension system does not have or will not develop a system of information security controls to maintain the integrity, confidentiality, and availability of public pension system data
- Management may not adequately communicate information security requirements to staff
- Information security can be breached by knowledgeable programmers/users
- Management may not adequately enforce information security controls
- Personnel responsible for securing information and IT hardware and software are not qualified and well-trained

- Individuals inside/outside public pension system could bypass information security controls
- Inappropriate use of override capabilities, allowing a person to avoid system edits designed to identify irregularities and cover-up fraudulent activity
- Computer hardware, software, data, and documentation may not be adequately protected from theft, vulnerabilities, or compromise
- Network and/or data is compromised
- Intrusions detection resources and processes are ineffective
- The program to manage patches for known system vulnerabilities is ineffective
- Storage media are not properly sanitized before disposal or transfer
- Sensitive data is not secured

2. Controls to mitigate the risks

- Create information security policies and procedures
- Communicate information security policies/procedures to all employees on a regular basis. This should be required as part of new employee orientation
- Create physical and logical security systems for existing and developing information systems
- Test security systems periodically (by independent company or by internal audits) and develop a secure testing environment that precludes alteration of live data
- Monitor the security detection system and reports regularly
- Develop an incident response plan with clearly defined staff roles and responsibilities, including communication with the media. Test the plan periodically, document results, resolve issues, and update the plan
- Limit access to modify security rules and policies of IT systems
- Limit access to sensitive data to only essential personnel
- Encourage IT staff to become certified in relevant areas
- Develop a vulnerability patch management program that ensures patches are applied consistently and timely
- Ensure that all storage media are sanitize adequately prior to disposal or transfer
- Ensure that sensitive information is always encrypted regardless of storage media used.
- Eliminate the use of social security numbers as the primary identifier in the computer system.

C. Data Center

1. Risks

- Equipment malfunctions or is destroyed
- Equipment maintenance schedule is inadequate or not adhered to
- System availability/malfunction reporting is ineffective
- Reporting of environmental changes is ineffective
- Environmental and physical protection of equipment is inadequate (e.g., fire, water, power, temperature)
- Unauthorized access to data center (e.g., vendors, non-essential personnel)
- Fund resources are not adequate to support business needs

2. Controls to mitigate the risks

- Plan to have an alternative equipment or alternative site available in cases data center equipment malfunctions or is destroyed
- Develop and adhere to routine equipment maintenance schedule
- Develop an robust notification system so that appropriate personnel is advised timely when an equipment is not functioning or environmental changes reach a certain level that could have an adverse impact on the equipment
- Test the notification system on a regular basis
- Ensure that uninterruptable power supplies, non-water fire suppression system, and water detection sensors, are available and used
- Ensure that there is an adequate system in place to regulate temperature and humidity
- Configure layout of data center to minimize the potential for negative environmental or physical impact to equipment
- Ensure the data center is physically safeguarded (e.g., security badge required, biometric authentication) and access is restricted to key personnel
- Evaluate list of individuals with access to the data center regularly to ensure such access is appropriate. Revoke immediately access of terminated employees
- Review data center access log regularly for unusual activity (e.g., entry after hours or weekends)
- Ensure the location of the data center is not clearly labeled
- Install surveillance cameras
- Review and evaluate resource utilization reports regularly
- Review and evaluate capacity reports regularly

D. Software Management

1. Risks

- Unauthorized use of software can occur intentionally or unintentionally
- Fines and penalties are incurred due to software violations
- Software purchased that requires annual fees is not used

2. Controls to mitigate the risks

- Ensure policy and procedures are in place to comply with agreements for use of licensed software
- Perform periodic software compliance review to ensure there are no violations (ideally performed by operational staff)
- Promote employee awareness of appropriate software usage
- Ensure the physical safeguard of software media
- Evaluate the usage and need for specified software regularly

XXIII. LEGAL SERVICES

1. Risks

- There is no charter that adequately defines the services to be performed by the in-house legal staff.
- There is no adequate in-house legal staff with appropriate training and expertise in laws and litigation affecting public pension funds
- Public pension system does not obtain adequate help from outside counsel when necessary
- Legal office does not provide adequate advice and consultation in the areas of membership, benefit entitlement, fiduciary responsibility, ethics, contracting, public records, open meetings, and investments (securities, real estate, and alternative investments) and does not provide adequate advice in drafting legislation, regulations, and policies
- Legal office does not provide adequate representation before administrative hearings, court cases and other legal actions

2. Controls to mitigate the risks

- Create a charter that adequately defines the objectives of the legal services unit
- Specify the experience and skills required for in-house legal staff
- Determine the skill sets and analyses to be obtained from outside legal counsel
- Develop remedial legislation to correct inconsistent or confusing language
- Develop administrative rules that accurately reflect the intended implementation of the statutory language

REFERENCES

Recommended Practices for State and Local Governments, Government Finance Officers Association, Chicago, 2001 (updated 2003).

AICPA Standards.

Assessment Guide for U.S. Legislative, Regulatory, and Listing Exchanges--Requirements Affecting Internal Auditing, The Institute of Internal Auditors Research Foundation, Altamonte Springs, Florida, 2002.

"CPA's Handbook of Fraud and Commercial Crime Prevention", AICPA.

Quality Assessment Manual, Fourth Edition, Institute of Internal Audits, Lew Burnham, CPA, and others, 2/2002.

Government Auditing Standards.

IIA Professional Practices Framework.

Management Antifraud Programs and Controls: Guidance to Help Prevent and deter Fraud; document was commissioned by the Fraud Task of the AICPA's Auditing Standards Board and a draft document has been jointly prepared by the Association of Certified Fraud Examiners and other organizations.

Report of the NACD Blue Ribbon Commission on Risk Oversight (Washington, D.C.: National Association of Corporate Directors, 2002.)

Sarbanes-Oxley Act of 2002.

The Report of the Committee of Sponsoring Organizations (COSO) of the Treadway Commission, Internal Control—Integrated Framework.

APPFA • P.O. Box 16064 • Columbus, OH 43216-6064
www.appfa.org