THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
OFFICE OF ETHICS, COMPLIANCE AND AUDIT SERVICES

1111 Franklin Street, 5th Floor • Oakland, California 94607-5200 • (510) 987-0479 • FAX (510) 287-3334

Sheryl Vacca
SENIOR VICE PRESIDENT
CHIEF COMPLIANCE AND AUDIT OFFICER

July 1, 2014

EXECUTIVE DIRECTOR SCHLIMGEN

Subject: Final Audit Report Retirement Administration Service Center Fraud Risk Assessment – No. P14A007

Attached please find a copy of the final report for Project No. P14A007 – Retirement Administration Service Center Fraud Risk Assessment. With the issuance of this final report, please destroy any previous draft versions. We very much appreciate the assistance provided to us by you and members of your staff during our review. If you should have any questions, please feel free to contact me at 510-987-9646 (e-mail: Matthew.Hicks@ucop.edu)

Matthew Hicks
Audit Director

Attachment

cc: Senior Vice President Vacca
Director Lorenz
Manager Cataldo
Contractor Weiss
Contractor Lafrance
Contractor Farrell
Contractor Sachs

UNIVERSITY OF CALIFORNIA
ETHICS, COMPLIANCE AND AUDIT SERVICES
OFFICE OF THE PRESIDENT
INTERNAL AUDIT SERVICES

RETIREMENT ADMINISTRATION SERVICE CENTER
FRAUD RISK ASSESSMENT

Advisory Service Project No. P14C007
February 2014

Work Performed by:
Steve LaFrance, Contractor
Noah Farrell, Contractor
Jeffrey Weiss, Contractor

Executive Summary

Introduction

As part of the University of California Office of the President (UCOP) 2013 – 2014 fiscal year internal audit plan, Internal Audit performed an advisory engagement to assess fraud risk within the Retirement Administration Service Center (RASC). The RASC supports members of the University as they transition into retirement and with life events beyond work (including University of California Retirement Plan (UCRP) retirement income, UCRP disability income, survivor benefits and UC-sponsored health and welfare benefits).

A fraud risk assessment (FRA) is a mechanism by which organizations proactively identify and measure their vulnerabilities to fraud and misconduct risk. This advisory engagement was a proactive measure by the RASC to understand their specific fraud and misconduct risks and performance of this engagement did not suggest any known instance or occurrence of fraud within the RASC. By understanding specific fraud and misconduct risks, the RASC can better manage and monitor that risk in order to help prevent, detect and respond to potential issues of waste, fraud and abuse. Each FRA is tailored to meet the specific needs and culture of the organization. A sustainable process is developed in order for the organization to identify, measure, manage and monitor their on-going risk to fraud and misconduct.

Objectives and Scope

Based on discussions with RASC management and information gathered from the organization, the objectives of the advisory engagement were to:

1. Identify current controls in place to mitigate potential risk of common fraud scenarios occurring within certain processes of the retirement service center, and
2. Recommend additional controls or data analytic techniques that could be implemented to detect or further mitigate fraud risk within the program

The scope of the advisory engagement included the following processes:

Retirement Operations

1. Processing retirement elections
2. Processing disability applications
3. Processing death cases
4. Maintenance to member accounts (including non-contributory accounts)
5. Processing Qualified Domestic Relations Orders

Retiree Insurance Program

1. Benefit and insurance payments
2. Establishing new member insurance accounts
3. Servicing existing member insurance accounts
4. Verification of eligibility for insurance coverage
5. Medicare Secondary Payer claims

Customer Service and Records Management

1. Customer service inquiry handling
2. Security of sensitive information (physical and IT)

Operational Compliance and Calculations

1. University of California Retirement Plan (UCRP) calculations
2. Processing of buyback and reciprocity requests
3. Retirement plan changes
4. Processing of UCRP minimum required distributions
5. Settlement agreements involving UCRP

Procedures Performed

To accomplish the consultation objectives and scope, the following procedures were performed:

1. Established the project foundation and prepared for the FRA workshop by obtaining an understanding of RASC department structure, processes and systems used.
2. Established a definition for fraud as it relates to the RASC (see Appendix C) and agreed upon a fraud risk rating criteria.
3. Facilitated a fraud risk assessment workshop with representatives from the RASC to identify potential fraud scenarios within the in-scope processes.
4. For each fraud scenario identified, utilized a defined risk rating criteria to assign an inherent risk rating based on the significance and likelihood of each scenario occurring; absent of any controls.
5. Identified controls in place to mitigate the significance and likelihood of occurrence of each fraud scenario and assigned a residual risk rating.
6. Based on workshop results, developed a list of fraud risks not mitigated to acceptable levels of residual risk and identified related recommendations to enhance controls.

Summary of Fraud Risk Assessment Results

The table below depicts the number of fraud scenarios identified during the workshop and how these scenarios were rated, according to the risk rating definitions in Appendix C.

	High (3.6 - 5.0)[1]	Medium (2.5 - 3.5)[1]	Low (1.0 - 2.4)[1]
Inherent Risk	6	24	2
Residual Risk	**0**	**10**	**22**

[1]*Refer to Appendix C for risk rating criteria*

RASC representatives indicated the most significant and likely scenarios, before considering mitigating controls in place, were:

1. Theft of member personally identifiable information (PII) such as social security numbers, addresses, date of birth, or other PII resulting in identity theft and reputational damage to organization. This could be performed by an employee or outside party.
2. An individual fictitiously requests a change of direct deposit account so that plan distributions of a legitimate member are diverted to himself.
3. An individual fictitiously requests a change of address so that plan distributions (lump sum and monthly) of a legitimate member are diverted to himself.

4. Falsified disability claims may be submitted.
5. Individual may be collecting disability and working (especially outside of CA).
6. Adding ineligible family members to the retiree system.

Several controls were identified which reduce the significance and/or likelihood of the aforementioned risks, including, but not limited to:

1. IT general controls restricting system access to confidential information (password requirements, periodic user access reviews, segregation of imaged medical records, etc.).
2. Authentication of members prior to accepting a change of address and automatic confirmation procedures when changes to physical address or direct deposit accounts are made.
3. Review procedures in place for disability claims, including internal and third party reviews.
4. Verification procedures performed by a third party when a family member is added to a plan.

As suggested above, the presence of internal controls within RASC business processes reduces the significance and likelihood of fraud occurring within the organization and its processes. After considering controls identified by RASC representatives, the following scenarios were left with the highest residual risk rating (note: all of the following were considered as having 'medium' risk as defined in Appendix C.):

No.	Risk Scenario	Related Gap
1.	Theft of member personally identifiable information (PII) such as social security numbers, addresses, date of birth, or other PII resulting in identity theft and reputational damage to organization. This could be performed by an employee or outside party.	Access is not adequately restricted to offices where records with PII are retained, departments have inconsistent policies on physically safeguarding records with PII, and PII may be sent electronically without being prevented or detected. In addition, there is limited visibility into which employees are viewing electronic records with PII. When employees are transferred or terminated, exit checklists are not consistently utilized to verify all physical and system access is modified accordingly, and updating access is dependent on the supervisor notifying several points of contact.
2.	Theft of organization assets or other's personal assets by an employee, former employee, or outside party.	
3.	Terminated/transferred employee may still have system or physical access allowing them to process fictitious transactions or steal PII.	
4.	A member or a spouse's death is not reported and they collect part B reimbursement for someone that is no longer living (or collect retirement payments).	The process to identify member deaths is fragmented and ineffective. The overall process is currently being reviewed by RASC management for improvement.
5.	Service credit, service pay, age, graduated eligibility, date of separation, or lump sum cash out flag	Changes to key member information (service credit, age, date of separation, etc.) by current RASC employees may be

	considering various tiers are inappropriately changed by a current or former RASC employee to increase benefits of self/relative/friend.	audited by the same employee that made the change, allowing for inappropriate or fraudulent changes going undetected.
6.	Bid rigging in exchange for kickbacks or gifts or to benefit relative that owns vendor.	None identified.
7.	Duplicate coverage of retirement benefits (employee rehired and still collecting retirement).	The process of tracking rehired retirees to determine whether their earnings are above the 43% threshold could be improved.
8.	Physical check stock is stolen and converted.	None identified.
9.	Individual may be collecting disability and working (especially outside of CA).	No audit process in place to verify member state of residence.
10.	Falsified disability claims may be submitted.	The mechanism in place to identify false claims is limited.

Summary of Recommendations and Deliverables

RASC Management should consider the following recommendations to further reduce the significance and/or likelihood of the identified fraud scenarios from occurring. The following recommendations are for management's consideration in developing action plans based on the identified fraud scenarios and gaps listed in Appendix A.

1. Implement consistent policies across RASC departments to restrict physical and system access to PII. Physical access to locations storing records with PII should be adequately restricted only to authorized personnel and PII sent electronically should be properly encrypted (with periodic monitoring to ensure this is happening). In addition, implement consistent termination checklists to ensure employees that are transferred or terminated have physical and system access removed.
2. Continue reviewing processes for identifying member deaths and taking appropriate action in a timely manner.
3. Revise the audit process for member information changes (service credit, age, date of separation, etc.) to ensure critical changes are reviewed by an independent person. The audit process should be risk based, meaning the highest risk transactions should be prioritized over lower risk changes.
4. Implement data analytic procedures to identify retirees earning above the 43% threshold.

Documentation detailing all fraud risk scenarios, risk ratings, controls, and gaps were provided to management. Refer to **Appendix A**. **Appendix B** provides a heat map depicting the inherent and residual fraud risks identified. **Appendix C** provides the definition used for fraud and risk rating criteria.

No management corrective actions will be tracked by Internal Audit as a result of this review.

Appendix A

Fraud Risk Assessment

Subprocess(es)	Fraud Risk Type	Scenario No.	Fraud Risk Scenario	Significance of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Control Description	Management Control Effectiveness High = 5 Medium = 3 Low = 1	Significance of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Overall Fraud Risk Level High = 5 Medium = 3 Low = 1	Potential Gap(s) / Recommendations
Processing Retirement Elections Processing Disability Applications Processing Death Cases Processing Qualified Domestic Relations Orders Customer service inquiry handling University of California Retirement Plan (UCRP) Calculations	External	6	Theft of member SSN, addresses or other PII resulting in identity theft and reputational damage to organization.	4.75	3.50	*Clean desk policy and spot check - All (excluding accounting) *Use rules for CRM tools to help predict data *Password reviews and revalidation (employees - reset twice a year) *Review of user access rights semi-annually by BIS *Safe file - secure file sharing for sending sensitive information *Required training on information security (annually) *Access to name search is restricted / controlled to appropriate users *Shredders located throughout offices *CRM access is restricted (by IP address) for staff to business hours only *Audit CRM comments that are not encrypted to ensure not including PII, personal information. *Segregate access of medical records within imaging system to select users. *Policy against transmitting PII via email	3.38	3.69	2.62	3.15	*Access to office / building where records are retained that are not RASC employees / walk ins (are not tracked) *Limited visibility to who has reviewed which records; system unable to track views. *Heavily dependent on paper *Inconsistent policies on clean desk (i.e., Accounting) *Lack of system monitoring of PII being sent unencrypted.
All processes	Asset Misappropriation	7	Theft of organization assets or other's personal assets.	2.83	3.91	*Physical access (badge) *Asset tagging for fixed assets and perform periodic physical inventory count *Clean desk policy (including locked desk) *Building security *Staff members ask non-uc visitors to wait in lobby area for an escort	3.00	2.44	3.31	2.88	*Access to office / building where records are retained that are not RASC employees / walk ins (are not tracked)
All processes	Asset Misappropriation	30	Terminated/transferred employee may still have system or physical access allowing them to process fictitious transactions or steal PII.	3.83	2.17	*Policy for changing or deleting user access *System access review twice a year by BIS and verify with manager / supervisor of each department to verify appropriateness of users and their access *User accounts expire after 180 days of non-activity *Employees anticipated to separate from the organization have termination of access (building and system) scheduled to be removed	4.00	3.36	2.15	2.76	*Lack of a standardized process for modifying access of RASC employees transferring to other departments to ensure access is modified accordingly (exit checklist). Recommended standardize exit checklist to ensure access is terminated. *Dependent on supervisor notifying several points of contact to cancel access to all systems
Processing Death Cases	External	5	A member or a spouse's death is not reported and they collect part B reimbursement for someone that is no longer living (or collect retirement payments).	2.89	3.25	*Utilize third party vendor (PBI) for reporting of spousal deaths. Report obtained weekly. Possible for spouse not to be reported timely. PBI is one to two months behind. Process to contact member if benefits have been paid to spouse following death (challenge with clawing back benefits). *Receive call ins from family as well as reporting from medical plan carriers regarding member and spousal deaths	3.90	2.50	2.62	2.56	*Death reporting is a fragmented process and is currently under review for improvement
All processes	Asset Misappropriation	20	Service credit, service pay, age (DOB), graduated eligibility (GE), date of separation, or lump sum cash out flag considering various tiers are inappropriately changed by a RASC employee to increase benefits of self/relative/friend.	3.67	2.25	*Daily audit report (includes user initials) capturing what changed from / to, and date of change. *Audit 100% of transactions to verify source document agrees to calculation or change processed.	3.27	2.86	2.25	2.55	*Auditors may have access to audit own changes (lack of SOD, completeness of audit). Recomment improved consistency of audit practices. Audit Practices should meet control standards appropriate to the risk. *Oversight / review of audit practice related to transactions made within system to ensure 100% of transactions have been reviewed. Practice not consistent across departments.
All processes	Corruption	28	Bid rigging in exchange for kickbacks or gifts or to benefit relative that owns vendor.	3.50	2.30	*Form 700 (state form) for employees at certain levels *Vendor bidding process with Procurement to issue RFPs	3.82	2.90	2.18	2.54	*None identified
Processing retirement elections	External	25	Duplicate coverage of retirement benefits (employee rehired and still collecting retirement).	3.42	3.27	*Report captures duplicate coverage of employee and retiree that is issued quarterly (report worked by Retiree Insurance) *Report of retiree making plan contributions (retirement team) *Form required to be completed at each location (campus) for rehired retiree and rely upon location to code rehired retiree accurately in system	3.54	2.38	2.62	2.50	*Tracking of rehired retirees and exceeding of 43% threshold (able to work up to 43%).

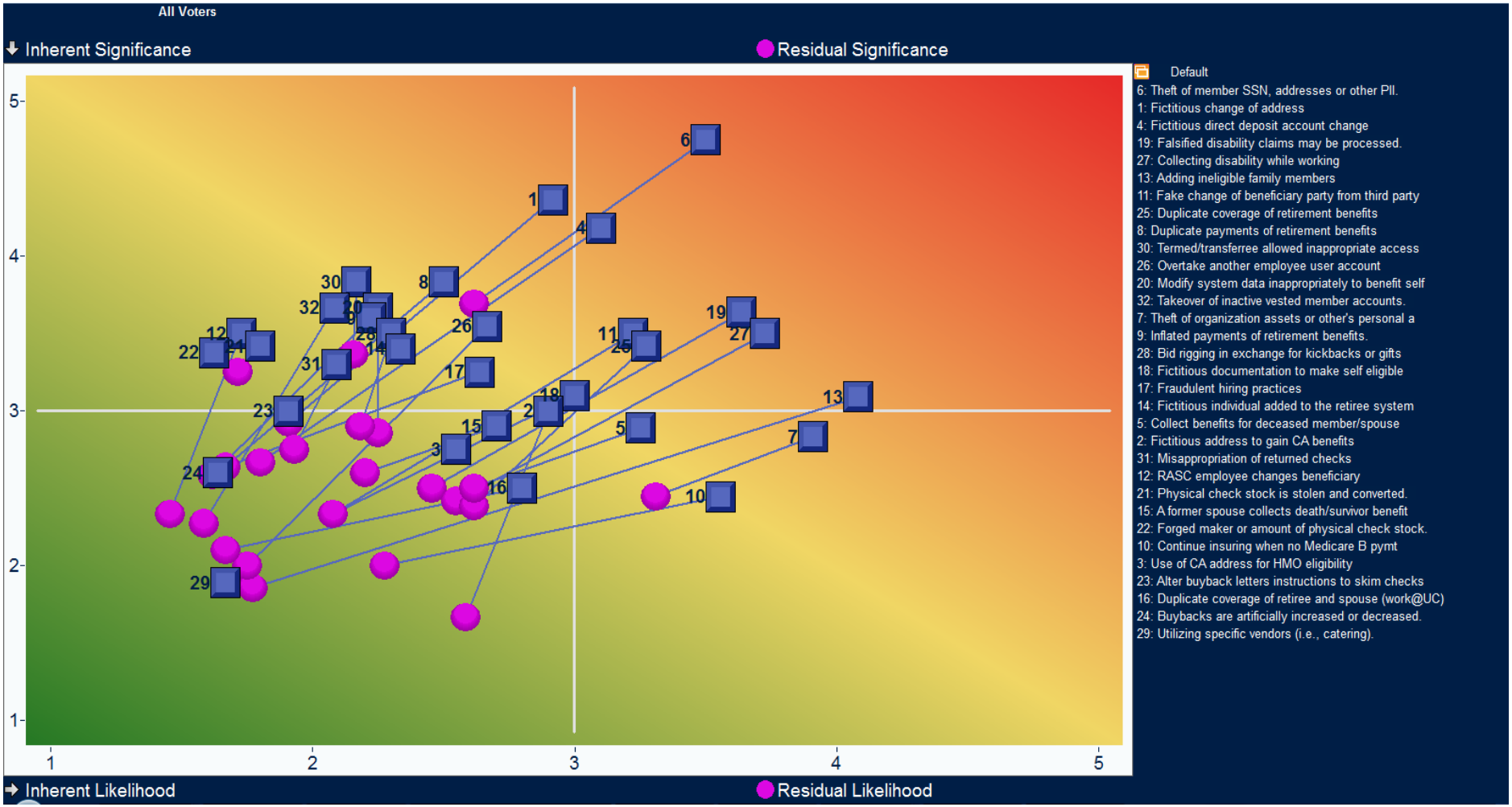
Subprocess(es)	Fraud Risk Type	Scenario No.	Fraud Risk Scenario	Significance of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Control Description	Management Control Effectiveness High = 5 Medium = 3 Low = 1	Significance of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Overall Fraud Risk Level High = 5 Medium = 3 Low = 1	Potential Gap(s) / Recommendations
Distribution payments	Asset Misappropriation	21	Physical check stock is stolen and converted.	3.42	1.80	*Positive pay controls via bank *Dual custody of check stock *Segregation between department responsible for custody of checks and printing of checks	4.62	3.25	1.71	2.48	*None identified
Processing Disability Applications	External	27	Individual may be collecting disability and working (especially outside of CA).	3.50	3.73	*For members in state of California, verify EDD information (quarterly)	3.30	2.42	2.55	2.48	*For members outside the state of California, reserve right to obtain tax returns but are not currently validating / or obtaining such returns. No audit process in place / sampling of members quarterly or annually
Processing Disability Applications	Asset Misappropriation	19	Falsified disability claims may be submitted.	3.64	3.64	*Hard review for first 12 months of disability claim *Medical releases / verify with Liberty Mutual that a claim exists *UCRP completed a review and identified members on disability that may not have had a claim or a claim was closed out and have Liberty do a re-review (initial one time project)	3.82	2.50	2.45	2.48	*Mechanism to identify false disability claims is limited (whether member is truly disabled - rely on Liberty and information from doctor)
Maintenance to member accounts (including non-contributory accounts) Processing Retirement Elections Processing Disability Applications Processing Death Cases Processing Qualified Domestic Relations Orders	Asset Misappropriation	1	An individual fictitiously requests a change of address so that plan distributions (lump sum and monthly) of a legitimate member are diverted to himself.	4.36	2.92	*Authenticate member when accept calls via customer service and ask member for three identifiers *Address change introduced through payroll and employee self service (active employees) *Utilize change of address form for members to request change *System (AYSO / CRM) sends an email or letter (to new and old address) to members upon processing of change. *Access to employees is restricted to change address / phone number. Employee unable to change member email address *Reporting to identify checks going to the same address (report development in progress) *Audit process where changes to system are reviewed to verify source documentation supports change	3.77	2.92	1.91	2.42	*Mail room has access to process change of address forms received (hard copy)
Processing Death Cases	External	15	A former spouse collects death benefit or survivor benefits.	2.90	2.70	*None identified	2.40	2.60	2.20	2.40	*Don't have verification process to verify spouse at time of death when spouse is receiving survivor benefits (marriage is established at time of plan setup)
Distribution payments	Asset Misappropriation	31	Misappropriation of returned checks, or utilizing knowledge that they are inactive for personal benefit.	3.30	2.09	*Process to record all checks returned on a tracker (Records Management). A CRM case is opened notifying Customer Service of check returned / to research. Checks are retained by Benefits Plan Accounting	3.17	2.75	1.93	2.34	* No control to prevent individual opening mail from misappropriating checks. Consider dual custody around opening of mail for returned checks
Maintenance to member accounts (including non-contributory accounts) Processing Retirement Elections Processing Disability Applications Processing Death Cases Processing Qualified Domestic Relations Orders	Asset Misappropriation	4	An individual fictitiously requests a change of direct deposit account so that plan distributions of a legitimate member are diverted to himself.	4.18	3.10	*Method to change direct deposit is restricted to 1) form (bank authorized or voided check - match name / address / printed check with member name) or 2) member logs into employee self service. *System (AYSO) sends an email or letter (to new and old address) to members upon processing of change. *Audit process where changes to system are reviewed to verify source documentation supports change	4.08	2.67	1.80	2.23	*For direct deposit change forms received; no letter or email to member confirming receipt of form and processing of change. Recommend validating & documenting direct deposit form procedures and assess need for member notification.
Processing retirement elections	External	11	Inappropriate change of beneficiary from an outside party through manually submitted request or online.	3.50	3.22	*Confirmation is issued to member upon processing *Retain history for all beneficiary changes *Beneficiary form requires PII to authenticate member *Upon reporting of death, member is blocked from accessing self service *Access to employee self service requires members to have a password	4.08	2.33	2.08	2.21	*Unable to locate hard copy forms for changes made to beneficiary prior to system implementation
All processes	External	18	Submitted documents for benefit eligibility are fictitious, unable to be authenticated, or missing.	3.10	3.00	*Audit 100% of transactions to verify source document agrees to change processed (review process of documents based on experience)	3.33	2.33	2.08	2.21	*Documents in another language may not be understood / authenticated
Processing retirement elections	Asset Misappropriation	8	Duplicate payments of lump sum retirement benefits or continuous payments.	3.83	2.50	*System restricts issuing of duplicate payments *Audit process for system and manually issued checks	3.80	2.64	1.67	2.15	*System is queued to issue a check and a manual check is generated (prior to system issuance)
All processes	Corruption	17	Fraudulent hiring practices (ghost employees, hiring relative, interview manipulation etc.).	3.25	2.64	*During on-boarding for employment; request I-9 for SSN verification *SSN mismatch reporting with PBI (third party) *Rely on controls at locations to validate identification of employee / processes around creation of new employees in system	3.55	2.64	1.67	2.15	*None identified

Subprocess(es)	Fraud Risk Type	Scenario No.	Fraud Risk Scenario	Significance of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Control Description	Management Control Effectiveness High = 5 Medium = 3 Low = 1	Significance of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Overall Fraud Risk Level High = 5 Medium = 3 Low = 1	Potential Gap(s) / Recommendations
Benefit and insurance payments	Asset Misappropriation	10	Continue giving insurance to members who have stopped paying Medicare part B premium.	2.44	3.56	*Policy in place that if member does not produce Medicare Part B / re-enroll; coverage is dropped. *Monthly report from each carrier notifying UCRP of who has dropped Medicare part B (retirement insurance). Report is worked and members are contacted.	4.00	2.00	2.27	2.14	*None identified
Benefit and insurance payments	External	2	An individual fictitiously reports living in CA to be eligible for UC group	3.00	2.90	*Rely on change of address controls *Rely on notification by third parties (HMOs) if members are receiving benefits outside state of California or vice versa.	3.25	1.67	2.58	2.13	*No controls in place to verify member location of residence within RASC. However, impact of cost differential between plans is low.
All processes	Asset Misappropriation	9	Inflated payments of retirement benefits.	3.60	2.22	Consolidated with scenario 20.	4.08	2.58	1.62	2.10	Consolidated with scenario 20.
All processes	Asset Misappropriation	32	Takeover of inactive vested member accounts.	3.67	2.08	*Authenticate member when accept calls via customer service and ask member for three identifiers *Address change introduced through payroll and employee self service (active employees) *Utilize change of address form for members to request change *System (AYSO / CRM) sends an email or letter (to new and old address) to members upon processing of change. *Access to employees is restricted to change address / phone number. Employee unable to change member email address *Audit process where changes to system are reviewed to verify source documentation supports change *Age 60 report run monthly and automated process to notify member to collect benefits	3.69	2.27	1.58	1.93	*RASC employees have access to view PII and may also know which members are inactive, allowing circumvention of controls.
Processing Retirement Elections Maintenance to member accounts (including non-contributory accounts)	Asset Misappropriation	12	Inappropriate change of beneficiary from a RASC employee.	3.50	1.73	*Confirmation is issued to member upon processing *Retain history for all beneficiary changes *Beneficiary form requires PII to authenticate member *Upon reporting of death, member is blocked from accessing self service *Audit 100% of transactions to verify source document agrees to change processed	3.77	2.33	1.45	1.89	*None identified
Benefit and insurance payments	External	16	Duplicate coverage of retiree who has spouse working in UC system as well.	2.50	2.80	*Report showing if duplicate coverage (Retirement Insurance) is run quarterly and member is followed up with to verify coverage	4.18	2.10	1.67	1.88	*None identified
All processes	Asset Misappropriation	26	Can gain access to password of employee enabling ability to perform actions under multiple accounts.	3.55	2.67	*Passwords are encrypted *Passwords are required to be changed 180 day (users are prompted) *Passwords are alpha numeric (8 character) *Clean desk policy includes locking computers	4.08	2.00	1.75	1.88	*None identified
Maintenance to member accounts (including non-contributory accounts) Establishing new member accounts (insurance)	External	13	Adding ineligible family members to the retiree system.	3.09	4.08	*Perform family member verification (continually) with a third party when a family member is added *System configuration to roll off family members once certain age is reached.	4.50	1.86	1.77	1.81	*Not verifying continued eligibility for spouses (especially in case of divorces)
All processes	Asset Misappropriation	14	Adding fictitious individuals to the retiree system.	3.40	2.33	Consolidated with scenario 17.	Did not vote	Did not vote	Did not vote		Consolidated with scenario 17.
Benefit and insurance payments	External	3	In order to be eligible for HMO medical plan, individual uses relative's CA address when they are an out of state resident.	2.75	2.55	Consolidated with scenario 2.	Did not vote	Did not vote	Did not vote		Consolidated with scenario 2.
Distribution payments	Asset Misappropriation	22	Forged maker or amount of physical check stock.	3.38	1.63	Consolidated with scenario 21.	Did not vote	Did not vote	Did not vote		Consolidated with scenario 21.
Processing buybacks and reciprocity requests	Asset Misappropriation	23	Personal checks or checks from outside institutions for buybacks or reciprocity agreements are diverted or skimmed (letters with instructions are altered).	3.00	1.91	"Audit 100% of transactions to verify source document agrees to change processed" "Segregation between departments responsible for calculating buybacks and accounting for checks received"	Did not vote	Did not vote	Did not vote		*Individual sending letters with buyback instructions could have inflated amount sent to own address (or P.O. Box) and then submit the correct amount to the proper address.

Subprocess(es)	Fraud Risk Type	Scenario No.	Fraud Risk Scenario	Significance of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Inherent Fraud Risk High = 5 Medium = 3 Low = 1	Control Description	Management Control Effectiveness High = 5 Medium = 3 Low = 1	Significance of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Likelihood of Residual Fraud Risk High = 5 Medium = 3 Low = 1	Overall Fraud Risk Level High = 5 Medium = 3 Low = 1	Potential Gap(s) / Recommendations
Processing buybacks and reciprocity requests	Asset Misappropriation	24	Buybacks are artificially increased or decreased.	2.60	1.64	"Audit 100% of transactions to verify source document agrees to change processed" "Segregation between departments responsible for calculating buybacks and accounting for checks received"	Did not vote	Did not vote	Did not vote		Not applicable - low risk.
All processes	Corruption	29	Utilizing specific vendors (i.e., catering).	1.89	1.67	Not applicable - low inherent risk.	Did not vote	Did not vote	Did not vote		Not applicable - low risk.

Appendix B

Heat Map of Fraud Risks (note: the numbers below correspond to the third column of the Fraud Risk Assessment in Appendix A above)



Appendix C

Definition of Fraud as it Relates to RASC

According to the Association of Certified Fraud Examiners (ACFE), fraud includes any intentional or deliberate act to deprive another of property or money by deception or unfair means. Fraud can be committed internally by employees or externally by customers, vendors, and other third parties.

The Institute of Internal Auditors defines fraud as:

> Any illegal acts characterized by deceit, concealment or violation of trust. These acts are not dependent upon the application of threat of violence or of physical force. Frauds are perpetrated by parties and organizations to obtain money, property or services; to avoid payment or loss of services; or to secure personal or business advantage.

Fraud Risk Type:

- Misappropriation of assets (e.g., theft, false billing schemes, embezzlement)
  - Theft of cash receipts
  - Theft of cash on hand
  - Fraudulent disbursements
- Corruption (e.g., conflicts of interest, bribery, or influence payments that can result in reputation loss)
  - Conflicts of Interest
  - Bribery (including kickbacks, bid rigging, etc.)
- External (e.g., members / customers [retirees, active employees, separated employees, local benefits offices], vendors, or other third parties fraudulently obtain economic benefit through identity theft, theft of contributions or distributions, or other means)

Note: Financial statement fraud was out of scope for the purposes of this project (i.e., intentional overstatement revenues, understatement of expenses, etc.)

Fraud Risk and Control Rating Criteria

Fraud risk may be assessed on both an inherent and residual basis.

- *Inherent Fraud Risk*: The risk to an entity, in absence of any actions management might take to alter either the risk's significance or likelihood.
- *Management Control Effectiveness*: The ability of processes, policies, and procedures to prevent, deter or timely detect the given fraud scenario.
- *Residual Fraud Risk*: The risk remaining to the entity, after management has taken action to alter the risk's significance and/or likelihood.

For the purposes of the risk rating once the fraud scenarios were identified, we utilized the criteria below.

Significance – The impact of a risk if it occurs. Factors to consider include:

- Materiality of the fraud that could be perpetrated to the overall organization.
- Potential impact of fraud on the organization's reputation.
- Potential regulatory or legal ramifications of fraud risk.
- Possibility that customer / member funds, processes, or employees could be involved in fraud.
- Likelihood that senior management would be involved in the fraud.

Descriptor	Significance Description
High	Long term loss of image, brand or reputation; requires public / regulatory disclosure; perpetrated by senior management; requires immediate executive management action and Board attention; substantial dollar loss
High / Medium	Business impact requires significant additional resources to mitigate (internal or external); executive management actively involved in issue remediation; immediate Committee on Compliance and Audit notification needed
Medium	Business impact may require (mainly internal) additional resources; changes required to processes to prevent reoccurrence; Committee on Compliance and Audit notified of fraud during periodic reporting; dollar loss is moderate
Low / Medium	Requires senior and middle management attention only; minor changes to business processes required; Committee on Compliance and Audit notification not required
Low	Insignificant business impact, which is easily mitigated by process owners; changes to business processes not required; dollar loss is minimal

Likelihood – The probability that the risk will occur. Factors to consider include:

- Complexity – The more complexity involved in a transaction, the more likely fraud could occur.
- Subjectivity – The higher the degree of human judgment involved in the transaction, the more likely fraud could occur.
- Susceptibility – Transactions that are susceptible to material error, omission, manipulation, or loss are more susceptible to fraud.
- Velocity – The higher the volume and size of individual transactions processed, the more likely fraud could occur.
- Geography – Certain cultural factors or smaller offices with limited segregation of duties increase the likelihood of fraud.

Descriptor	Likelihood Description[1]
High	The risk is expected[1] to occur at least once in a 1 year horizon
High / Medium	The risk is expected[1] to occur at least once in a 3 year horizon
Medium	The risk is expected[1] to occur at least once in a 5 year horizon
Low / Medium	The risk is expected[1] to occur at least once in a 20 year horizon
Low	The risk is not expected[1] to occur in a 20 year horizon

[1] *Expected meaning greater or equal to 50% chance of occurring*

Management Control Effectiveness Rating Scale

Descriptor	Control Effectiveness Description
High	Mitigating controls reduce significance and/or likelihood to an overall low fraud risk
High / Medium	Mitigating controls reduce significance and/or likelihood to an overall low / medium fraud risk
Medium	Mitigating controls reduce significance and/or likelihood to an overall medium fraud risk
Low / Medium	Mitigating controls reduce significance and/or likelihood to an overall high / medium fraud risk
Low	Mitigating controls do not reduce significance and/or likelihood of fraud risk