PETER HUGHES, Ph.D., CPA, CIA, CFE, CITP
Director

400 Civic Center Drive West
Building 12, Room 232
Santa Ana, California 92701-4521

(714) 834-5475 Fax: (714) 834-2880

INTERNAL AUDIT DEPARTMENT

File No. 2247

March 27, 2003

TO: David E. Sundstrom, Auditor-Controller
Jan Walden, Assistant CEO/Human Resources
Daniel Hatton, Assistant CEO/Information and Technology

SUBJECT: Report on Risk Assessment for County Accounting and Personnel System (CAPS) Payroll Application, File No. 2247

Attached is a copy of our report on Risk Assessment for County Accounting and Personnel System (CAPS) Payroll Application. If you have any questions, please call me or Eli Littner, Deputy Director, at 834-5899.

Respectfully submitted,

Dr. Peter Hughes, CPA
Director, Internal Audit Department

Attachment

Other recipients of this report:
Members, Board of Supervisors
Members, Audit Oversight Committee
Foreman, Grand Jury
James D. Ruth, Interim County Executive Officer
John Nakane, Chief Assistant Auditor-Controller
Jim McConnell, Assistant Auditor-Controller, Central Operations
Shaun Skelly, Assistant Auditor-Controller, Agency Accounting
Larry Chanda, Manager, A-C/CAPS Administration
Mahesh Patel, Assistant Auditor-Controller, Information Technology
Jim Berch, Accounting Systems Manager, Auditor-Controller
Ray Stephens, Payroll Systems Lead, Auditor-Controller
John Wheeler, Information Systems Manager, CEO/IT
Susan Paul, Employee Relations, CEO/HR
Marguerite Adams, Corporate HR Services, CEO/HR
Scott Sanders, Sr. Systems Analyst, CEO/HR
Phil Paker, ACS State and Local Solutions

RISK ASSESSMENT FOR COUNTY ACCOUNTING AND PERSONNEL SYSTEM (CAPS) PAYROLL APPLICATION

March 27, 2003

File No. 2247

Technical Expert: John VanBorsum, iSecurePrivacy

Other Internal Audit Department Contributors:
Peter Hughes, Ph.D., CPA, CIA, CITP
Eli Littner, CPA, CIA, CISA
Autumn McKinney, CIA
Dan Melton, CPA
Leigh Riddle, CIA
Scott Suzuki, CPA, CISA

Internal Audit Department

RISK ASSESSMENT FOR
COUNTY ACCOUNTING AND PERSONNEL SYSTEM (CAPS)
PAYROLL APPLICATION

Table of Contents

Executive Summary 1

Introduction 1

Risk Management Conclusion 1

Vulnerability Assessment 1

Summary of Findings 2

Audit Scope and Approach 4

Scope 4

Approach 4

Acknowledgement 5

Observations 5

Detail Observations 6

1. Application Recovery Plan Inadequate For CAPS and CAPS Payroll 6
2. Recalculated Payroll Processes with Only Minor Discrepancies 7
3. System Access to Production Datasets Bypassing Application Control 7
4. 28 User Names Have Application Access to *ALL Payroll Tables 9
5. Premium Pay Input is Decentralized and Prone to Error 10
6. Basis for Computing Unemployment Reserves 10
7. Published Title Table Appears Out of Date 12
8. Medicare Differences and Non-Payments 12
9. Application Security Profiles are Deployed 13
10. Dialog Between Human Resources, Auditor-Controller, and Information Systems 14

Management Response 15

Executive Summary

Introduction

In July 2002, the Internal Audit Department contracted with iSecurePrivacy, a professional consulting firm, to assist them in assessing the risk within the County's payroll processing. County payroll is processed on the County Accounting and Personnel System (CAPS). This application is vendor-provided by American Management Systems. The Advantage application is widely used by government entities. The County currently uses Advantage 2.2 for its payroll application. The Auditor-Controller's Office supports the CAPS application internally through Functional Analysts who perform production processing table maintenance, ensure payroll processing is correct, and develop business requirements when changes to the software are required. ACS is the third party vendor that develops application modifications in concert with the County's requirements.

The Internal Audit Department contracted with iSecurePrivacy to assist in evaluating the risk in the County payroll process. A comprehensive application risk review such as planned has not been performed before. The County's payroll process is complex. The employee staff exceeds 19,000 individuals many of whom are paid in accordance with various union contracts. Most workers are hourly employees with numerous incentives and premium pay categories as options.

Our fieldwork was performed during six weeks in October and November 2002. We worked extensively with the biweekly payroll cycle ending August 30, 2002. This cycle is one of two cycles each year where three pay days occur in the same month, and not a biweekly payroll with the typical benefit deductions.

Risk Management Conclusion

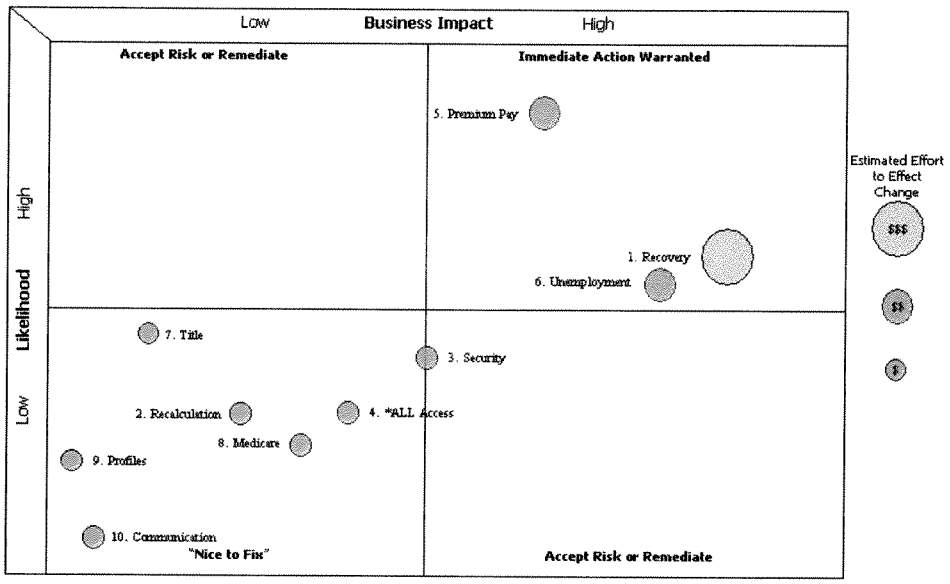
Based on our review, we noted a high degree of professionalism and knowledge within the information systems staff. These individuals are a key part of the system of internal control and risk management function. Largely because of their dedication, we found that the payroll application presents a LOW level of business risk to the County. We identified an issue involving application recovery planning that would normally raise the level of risk; however, this issue is not totally under the control of the Auditor-Controller CAPS Payroll function and we are not elevating the overall risk evaluation due to this single factor.

Vulnerability Assessment

Below on page 2 is a pictorial summary of our observations.

We recommend necessary action to be taken related to its observations based on the perceived risk. If an issue is in the upper right quadrant of the graphic, we believe the risk is significant and the County needs to take immediate action to repair the deficiency. For observations whose risk places them in the upper left or lower right quadrants, we suggest the County formally evaluate the risk and make a conscious decision to accept or to repair the vulnerability. We suggest the evaluation be documented since we are often unaware of the business case supporting a practice or future plans that might increase risk of the issues categorized in the upper left or lower right quadrants. For observations located in the lower left quadrant, we classify these as "nice to fix" issues but they should not require the immediate action or formal evaluation of the other three quadrants. These items also show areas where management demonstrates a significant control process that has a positive impact on organization risk.

Vulnerability Assessment



Summary of Findings:

Vulnerability Assessment	*Vulnerability Description*
1. Recovery	Application Recovery Plan Inadequate For CAPS And CAPS Payroll The County's application recovery plan shows a lack of preparation to respond in case of a significant power outage or unavailability of the data center.
2. Recalculation	We recalculated Payroll Processes With Only Minor Discrepancies Only 41 employees (0.2%) seemed to have differences between hours input and gross pay. In researching them, we concluded the majority were the result of bad input detected within payroll processing. We were able to verify that system calculations appeared accurate with isolated, minor exceptions.
3. Security	System Access To Production Datasets Bypassing Application Control We found 61 business users who have TSO UPDATE access to production datasets thereby bypassing application controls.
4. *ALL Access	28 Users Have Application Access to *ALL Payroll Tables Only four of these have UPDATE access to all tables, but the others can inquire against virtually all payroll and human resource information.

Vulnerability Assessment	*Vulnerability Description*
5. Premium Pay	Premium Pay Input Is Decentralized And Prone To Error The County's business model decentralizes much of the staff setup and maintenance. We found some errors that could put the County out of compliance with OCEA Memoranda of Understanding.
6. Unemployment	Basis For Computing Unemployment Reserves The County is self-insured for unemployment. We noted that the rate used is significantly lower than for employers who participate in State and Federal unemployment programs.
7. Title Table	Published Title Table Appears Out Of Date We found almost 2,000 staff whose CAPS payroll title were not found in the title table dated 8/2/2002. Titles are critical to payroll processing and we believe the published table is out-of-date.
8. Medicare	Medicare Differences And Non-Payments We found discrepancies in 0.48% of Medicare payments of +/- $0.20. We also found 285 staff that were not having Medicare withheld (this is not necessarily a processing error as some County employees are exempt from Medicare taxes).
9. Profiles	Application Security Profiles Are Deployed This is a best practice and seems to facilitate administering user security. We noted there are a large number of profiles and this could make them difficult to manage.
10. Communication	Dialog Between Human Resources, Auditor-Controller, and Information Systems Communication is critical to controlling a process as complex as the County's payroll. We observed evidence of significant interaction among these groups.

Audit Scope and Approach

Scope

We reviewed payroll processing for Cycle 18 of 2002. This cycle produced the checks issued on August 30th and Cycle 18 is the third processing cycle in the month of August. August is one of two months in 2002 in which three payroll cycles occur. The County processes payroll on a biweekly basis and deductions for employee health, dental, and life insurance are not taken on the third payroll cycle within a month.

- Our review included non-monetary as well as monetary processing within the CAPS payroll application.
- We recalculated hours to gross pay and gross pay to net pay.
- We sampled premium pay to determine it was being paid in accordance with Orange County Employee Association Memoranda of Understanding.
- We evaluated security for payroll application datasets and transactions including interface files that transmit payroll information to financial institutions.
- We verified our work against production reporting to determine if we could reasonably reconcile our recalculation results with production results.
- We did not research all discrepancies, because that was outside our scope given the complexity of the County's payroll. We did provide the identified discrepancies to Auditor-Controller staff for resolution.

Approach

We reviewed non-monetary, monetary, and infrastructure risks within the payroll application by performing the following analytic processes:

- Recalculating Payrolls – determine payroll processes are in concert with management expectations and labor contract agreements.
- Determining Data Integrity – review selected data elements to determine if application editing is sufficiently robust to prevent unexpected processing results.
- Reviewing Infrastructure – determine if the overriding technology environment evidences contemporary controls.
- Evaluating Security – evaluate whether controls are present to reduce the likelihood of staff payroll being inappropriately disclosed or intentionally manipulated.

With the help of ACS, we obtained a copy of the CAPS payroll "PCEF" file (HR30P) that contains the results of payroll processing. We were also provided with various input files including 1Pay Transactions (HR10N), Mileage Transactions (HR10P), Manual/Keypunch Time Sheets (HR30A), and Virtual Time Sheets (HR32A).

We reconciled our PCEF file to the production Payroll Register Report (HR31G10-1) obtained from ERMI online reports. The audit PCEF file summed to a total of $40,319,295.40 for Gross Pay and was $1,899.13 more than the Payroll Register Report. Upon researching this, we determined that the PCEF file provided to us did not contain cancelled check transactions. We identified the extract program problem, but decided this difference was not material – representing less than 0.005% of the total payroll.

Acknowledgement

Throughout our engagement, we informed the County of issues we detected. The business units responded in a positive and timely manner. Throughout the project, all County and contractor individuals staff contacted were extremely helpful and forthcoming with available information. We would like to thank the Auditor-Controller staff, CEO/IT staff, and ACS staff for their support and cooperation during the audit including: David Sundstrom, CAPS Executive Sponsor, Jan Walden, CEO/Human Resources Director, Larry Chanda, A-C/CAPS Project Manager, Phil Paker, ACS CAPS Manager, Mahesh Patel, A-C/Systems Division Manager, Anthicom Parinayakosol, ACS HR Team Lead, Scott Sanders, CEO/Human Resources Senior Systems Programmer Analyst, and especially Ray Stephens, A-C/CAPS Payroll Systems Team Lead.

Observations

Detail Observations

The following section discusses the business risks shown in the vulnerability matrix on page 2.

1. **Application Recovery Plan Inadequate for CAPS and CAPS Payroll**

Information technology is a critical component to County services. All technology processes are vulnerable to outages and need predefined actions that routinely take place to protect against a protracted period of system unavailability. We were provided with the County's Agency Application Recovery Team Plan (updated January 15, 2002). Several pages are devoted to CAPS, which is recognized as mission critical for delivery of County services.

Observation:

We noted the County does not have a backup data center available. Should its data center be destroyed or suffer a catastrophe that makes it inaccessible, it would be extremely difficult to resume services in a timely manner. Not having a backup site available means that there has never been a test of completely restoring the mainframe-processing environment from backups. Moreover, pointing out that daily backup files are typically stored on site within the data center rather than at a remote location. This exposes the County to significant risk in the event of a data center catastrophe.

Recommendation:

The County needs to enhance its application recovery plan and evaluate its risks from a significant CAPS outage. It should also be pointed out that the current application recovery plan addresses only the mainframe environment. Restoring communications, obtaining access to system documentation at the Civic Center facility, and agency/department records needed to process CAPS payroll also need to be addressed in a comprehensive recovery plan.

Management Response:

Partially Concur - It is correct that the County does not have an identified backup data center – or "Hot Site". We have investigated this option and believe that the costs are too great and cannot be justified given the level of risk and the current budget situation. However, we do believe that it is an important element of disaster recovery.

To address this issue we will explore possible lower cost options such as, a backup site provided by our major outsourcer ACS or a partnership with other California counties to provide mutual backup. To be complete by June, 2004.

It is correct that daily backups are stored on-site. However, weekly data center backups are stored off-site. These back-ups are sufficient to restore and run the CAPS system. The Data Center has a documented disaster recovery plan to restore the system from these backups at our site. The County considers that potentially losing several days of work is an acceptable business risk. We do not concur with this part of the recommendation.

The Auditor-Controller has developed a plan that addresses generation of payroll checks should a disaster occur. It calls for creating a standalone process using information from the prior payroll to create either hardcopy checks or electronic payments. This process will be developed and tested as part of the CAPS upgrade project.

2. **Recalculated Payroll Processes With Only Minor Discrepancies**
County payroll is a complex process that involves a significant amount of information to verify. Using audit software we tested the hours to gross pay calculation, overtime payments, reimbursement payments, deductions, and the calculation of net pay.

Observation

We found 41 (out of 20,025 – 0.2%) employees in which the time sheet hours input to CAPS were different from the hours used to calculate gross pay. Based on our research into these differences, we were able to conclude the majority was due to bad time sheet data that was detected and corrected prior to producing paychecks. This shows the County's internal review process is functioning in a reasonable manner.

We recalculated overtime pay and found no discrepancies from the results expected. We verified and summed reimbursement amounts and determined they were correctly reflected in the paycheck information. We sampled and determined that quarter-to-date fields in the payroll application were accumulated correctly. We were able to recalculate Federal and California income tax withholding amounts.

We were able to determine that deduction amounts were correctly calculated based on information provided by the County. The area of retirement contribution is complex and we did not actually review retirement plan documents to ensure they were accurately recorded onto the summary documents we used for this test.

We were unable to perform any substantive testing of "1Pay" transactions. These are corrections or retroactive payroll transactions that are manually determined and input to the application. The 1Pay transactions basically only provide the amount of the entry without the derivation of the hours or amount fields. We learned that a project earlier in 2002 was established to evaluate automating these transactions, but in light of the cost and the CAPS Upgrade project, it was cancelled.

Recommendation:

We believe the payroll process overall has integrity and results in accurate and timely paychecks being produced. We have no recommendations to improve this process.

3. **System Access To Production Datasets Bypassing Application Control**
Application security can be bypassed if an individual has direct system access to production datasets via IBM's Time Share Option (TSO) capability. Within the IBM environment, datasets are defined as resources and protected at the County using IBM's Resource Access Control Facility (RACF). CEO/IT Data Security Administration manages mainframe access controls within the data center.

Observations

Access to the direct deposit files (automated clearing house files transmitted to Wells Fargo or Orange County Federal Credit Union) is controlled through RACF. The user profiles authorized to access these files is limited to what appears to be an appropriate number. We believe the County's risk of an unauthorized individual manipulating these critical files is low.

Based on our review, the County has a policy for password security that is laudable in its password construction and change frequency.

A. We reviewed RACF security profiles for all payroll/human resource datasets (defined with the high-level qualifier PHR). We detected instances of access to production datasets that appear to be inappropriate. There are 61 staff members with ALTER access to production input datasets (largely for Virtual Time Sheet files). ALTER is a more privileged state than UPDATE or READ. It allows staff to delete entire datasets among other capabilities. This is contrary to management's policy of restricting users to only those capabilities required to perform job duties. In our discussions with local security administrators, we were informed they had tested the need for ALTER and found that UPDATE appeared to be sufficient for the VTI function.

B. Within this 61, we noted 11 userids with UPDATE or ALTER accesses that appear to be functional analysts (based on the County's user naming convention). This could violate the County's mainframe security policy of restricting application programming and maintenance personnel to READ access.

C. We found a Group Access profile of MMFINREC that has UPDATE access to several production datasets. At least one member of this group has an application programmer userid. When we discussed this with ACS's Application Systems & Programming Manager, we were informed this was a previous entitlement and it should be removed.

Recommendations:

A. We recommend the local security administrators for CAPS complete their assessment for ALTER access to the Virtual Time Sheet datasets. Unless it is found that the application architecture requires this level of access, it should be removed.

B. We recommend that access privileges to production datasets be evaluated to determine if access is appropriate for functional analysts. We anticipate that the CAPS Upgrade will help to address this issue because it is table-driven by design allowing tables to be updated through application processes rather than system access.

C. We recommend that MMFINREC access group be reviewed to ensure that all users within the group require UPDATE access.

Management Response:

A. Concur – Completed January, 2003. All VTI timesheet datasets have been converted from ALTER to UPDATE for agencies and department personnel.

B. Concur – Access to production datasets will be reviewed for appropriateness during the upgrade project. Estimated completion 2nd quarter, 2005.

C. Concur – Dataset UPDATE access for the MMFINREC access group will be reviewed for appropriateness and exceptions corrected. Estimated completion 2nd quarter, 2003.

4. **28 User Names Have Application Access To *ALL Payroll Tables**

Local security administrators (LSA) within the Auditor-Controller's Office oversee payroll application security. LSAs are responsible for setting up new application users and modifying user access upon receipt of authorization from management. Access to payroll requires there to be a valid mainframe user name (RACF) as well as being included in the application tables themselves.

Observation

In reviewing application security tables, we noted 28 user names that have access to all application tables (*ALL). This represents 3.3% of the CAPS human resource sub-system. The CAPS application deploys a further restriction that access is defined as either update or inquiry, which mitigates this risk. The Local Security Administrator explained that only four user names have UPDATE access and the *ALL capability. Three of these four are members of the Auditor-Controller's information systems group and, given their current accountabilities, this access appears appropriate.

The fourth, ACUS563 user name, is used for emergency application changes and is well controlled among the A-C Information Systems Group, ACS Applications Systems & Programming, ACS Computer Operations, and the ACS Help Desk. We were satisfied that management control for ACUS563 is sufficient.

A best practice limits users to privileges required to perform authorized duties. The County appears to have limited application access in a prudent manner.

We were informed that security reporting from the CAPS application is limited to table maintenance. While the administrative security control appears sufficient, an unmonitored control may turn out to be critical. For example, no reporting is available to document activities of users with the *ALL update access.

Recommendation:

We recommend the A-C Local Security Administrator determine what, if any, security event reporting could be implemented. We also suggest security monitoring be a defined task within the CAPS Upgrade project that is just beginning.

Management Response:

Concur – Critical Reference Tables in the Human Resources system have been logged, and reported to functional administrators on a daily basis, since the system's inception. The SLOG feature will be evaluated for usefulness in monitoring security events and deployed if found to enhance security beyond what is available from RACF. Estimated completion of SLOG evaluation 2nd quarter, 2003.

5. **Premium Pay Input Is Decentralized And Prone To Error**

Depending on the Memoranda of Understanding (MOU) and job functions, individuals working at the County are eligible for additional pay depending on skills or work environment. There are more than 50 codes used to capture this pay. It must be entered on the CAPS ESMT employee setup screen. The data entry involves entering the correct code as well as the correct rate – this rate can either be a dollar amount or a percentage.

Observation

We sampled and found 36 staff who were receiving premium pay inconsistent with the MOU. Twenty-seven of these were being underpaid for Jail Assignment duties based on the MOU (difference of $.58 per hour).

The remaining nine in the sample were receiving premium pay that the MOU does not specifically authorize. In these cases, the pay might be authorized due to extenuating circumstances, but that information is not available within the application database.

We were informed anecdotally that bilingual pay is often paid at an incorrect rate, especially after a staff member's duties change.

Recommendation:

Since premium pay has a contractual basis, we would recommend that Human Resources conduct a study of all premium pay to ensure conformance with the MOU. We further recommend that the CAPS Upgrade project address this issue as an opportunity to improve control and streamline workflow when establishing or changing an employee's status.

Management Response:

Concur - Starting in approximately late Fall 2002 CEO HR Records began to audit premium pay that includes ensuring any errors found being corrected. This along with reports that Departments have to help them identify/correct any errors plus an online procedures manual (in development) will provide resolution to the issues noted relative to premium pay input being decentralized and prone to error. Also there is one bi-lingual rate code (BL) for which multiple rates are possible, which makes auditing of this code more difficult. We are looking into establishing a unique bi-lingual code for each unique rate which should thereby make auditing this function easier.

6. **Basis For Computing Unemployment Reserves**

The County self-insures for unemployment benefits for staff terminating employment in a situation that would allow them to claim benefits. The rate used is 0.08% with no cap on wages (subsequent to this audit date, the County rate was increased to 0.15%). This amount is paid by the County and is not an employee responsibility. For employers paying into the California Unemployment Insurance Fund, the rate is between 0.7% and 5.4% depending on the employer's experience. The Federal Unemployment Tax rate is an additional 0.8% for employers.

Observation
We noted the County's unemployment insurance reserve rate is significantly below that of organizations covered by State and Federal agencies. The County does not cap its unemployment payment (which is set at $7,000 for both State and Federal), and that could make a difference in the amount that is actually held in reserve.

We estimated the annual salary of an average County worker to be $35,000. Using that rate we estimate the County's unemployment reserve would be $52.50 ($35,000 * 0.15%) per employee. Under the State and Federal programs, the County's unemployment contribution would be $105 per staff member ($7,000 * 1.5%), assuming the County's experience with unemployment would put it in the lower echelon of government payments.

Recommendation:
We recommend that the experience and rate assumptions used by the County to determine its unemployment reserve be reviewed and validated as accurate.

Management Response:
Do not Concur - The current unemployment premium rate of .0015 is developed to fund the annual unemployment claims paid as a direct reimburser through the State Employment Development Department for unemployment benefits. It is not a reserve, nor does it have any portion of the rate designed to fund a reserve. Current retained earnings are sufficient to fund a reserve necessary to pay future base period claims.

Projected claims are determined using analysis of average quarterly claims costs over the last 12 months period, adjusted to reflect 1) changes in unemployment benefits or length of claim as mandated by legislation and 2) increases or decreases in quarterly claims cost due to changes in the overall labor market due to the economy and/or changes in the County turnover rate.

Recent changes in the legislation increasing the weekly benefit amount and length of claim were factored into the current rate however global economic conditions and reductions in County workforce due to the budget crisis could impact future claims. As unemployment claims increase either due to increased length of claim or due to an increase in the number of claimants, the current rate of .0015 may need to be adjusted.

However as pointed out in the internal audit observation above, at the current time, the existing method of self funding as a direct reimburser is much less costly than participating in the State fund as a tax rated employer. In fact, the County currently contracts for administration of unemployment claims management with Gates McDonald through a consortium of other California Counties known as the County Personnel Administrator Association of California, CPAAC. Participation with the CPAAC consortium provides the advantages of combined efforts on legislative action, pursuit of recovery of state mandated expenditures, sharing of consortium data and having input into the state on administrative regulations.

Also, as a clarification, our records show that the estimated salary of an average County employee is approximately $50,000 rather than $35,000.

7. **Published Title Table Appears Out Of Date**

The County maintains a large number of position titles that govern payroll processing. This information is formally published on the County's Intranet and available to employees.

Observation

We obtained a copy of the Title Schematic by Title Code as of August 7, 2002. We compared that published document to the title information found in the payroll application.

We were unable to find 1,971 employee titles in the published title table. In discussing this with the A-C's payroll functional analyst, we were told that titles drive the payroll process and something must be wrong with the published table.

We also found 91 staff whose pay rate exceeded the maximum hourly rate found in the Title Schematic. These are probably authorized exceptions that are approved by Human Resources due to special needs or skills. However, we could not determine this from the application database.

Recommendation:

We recommend this finding be researched and the Title Schematic be updated on the web site, if necessary. We also suggest that the 91 staff be reviewed to ensure they are authorized for rates above the table maximums.

Management Response:

Do not Concur - Although noted by ISecurePrivacy that their findings included almost 2000 staff with a title not found in a title table dated 8-2-2002 we believe that ISecurePrivacy may have been provided with a title schematic dated 8-2-02 which specifically applies to the County titles and not the full titles that are in AHRS which includes other entities such as the Courts and special districts.

8. **Medicare Differences And Non-Payments**

The issue of Medicare is a complex one for the County. The standard rule is that employees starting County service prior to May 1, 1986 cannot be required to pay Medicare. The issue is more complex because staff can use employment with other state and local governments to establish their employment date. The payroll application does not retain the actual hire date in its static data – instead it uses an "appointment date" as a reference date.

Observation

We found 285 staff that were not having Medicare withheld from their paychecks. This also means the County is not paying the employer portion of Medicare. We tried to determine if this number was appropriate but were unable to find a systematic way of determining "government service" date. We were informed that it would require a manual review to ensure each employee is correctly coded. This was beyond the scope of this audit. During the audit, payroll systems personnel produced a similar list and began a process of review. Corrective action is being taken to verify coding for these employees.

We also found discrepancies in the amount of Medicare tax being collected. We found 79 (out of 15,579 – 0.48%) whose Medicare computation was +/- $0.20 of the expected amount. We do not consider this to be a significant risk to the County.

Recommendation:

We believe, based on representations from County staff, that appropriate action is being taken to resolve these employee Medicare issues.

Management Response:

Concur -The Auditor's Office/Central Payroll Section is currently reviewing our listing of potential Medicare discrepancies, which will result in corrective action being taken to ensure that eligible employees are being subject to the Medicare tax. Additionally, action will be initiated requiring that a biweekly report be generated for the purpose of identifying potential Medicare issues in a timely manner. Estimated completion is 4th Quarter 2003.

9. **Application Security Profiles Are Deployed**

Establishing user profiles is the best practice when managing a large user base. In the case of the CAPS human resource application, there are more than 800 user names authorized for some functionality within the application. Of these, 125 are associated with CAPS payroll functions.

Profiles can be efficient in setting access privileges because they do not require the security group to uniquely define every user. There are 83 individually identified profiles in the human resource application, and 14 with payroll functionality.

Observation

We noted 34 user names that do not belong to a defined profile. This means their table access is defined individually reducing the efficiencies obtained through profiles. Of these, 25 have access to *ALL tables. This indicates that profiles (the preferred method of administering application security) is the predominate manner of assigning application security.

A. We observed that 34 profiles have only one or two members. This in effect makes them a unique profile and increases the complexity of managing the profiles. The profile naming convention is helpful in determining what the profile is authorized to do and this is sufficient reason to retain these relatively unique profiles.

B. We found one user name (PEUS004) with a profile of SPECIAL. We also found one user name (HCUS030) with a profile of NONE, which is in the *USE security group only. Upon discussing this with CEO/IT Data Security Administration (RACF security management), we were told that PEUS004 and HCUS030 are not defined to RACF. This most likely means they should be deleted from the CAPS application security table.

C. We were also informed that the process for reviewing user names who may have transferred or terminated is not an automated task. There is a control provided in the County's user naming convention. The first two characters of a userid denote the agency or department in which the individual resides. Individuals, by policy, can only have one userid and when a transfer occurs, they receive a completely new userid. This might effectively control users transferring from one agency or department to another, but may not address segregation issues when an individual transfers within the same organizational entity.

Recommendation:

A. We believe there are opportunities for creating additional efficiencies within the application security group by evaluating the need for so many profiles. We recognize this is not a trivial task, and suggest it be accomplished during the CAPS Upgrade rather than undertaken within the current environment.

B. We recommend the PEUS004 and HCUS030 user names be researched and deleted as appropriate.

C. We recommend implementation of a security capability to notify local security administrators in a timely manner when a staff member transfers or terminates.

Management Response:

A. Concur – A limitation within the Advantage 2.x product will not allow granting of multiple profiles to an individual. This limitation requires the need to create unique profiles for some users who are authorized for several access types (e.g., budget and HR). It is our understanding that the Advantage 3.x product allows the assignment of multiple profiles to an individual which should alleviate the need to have unique profiles. This issue will be addressed in the upgrade project.

B. Partially Concur – PEUS004 RACF ID. The User ID's contained in the AHRS security tables are periodically reconciled to RACF and discrepancies resolved. PEUS004 was a valid ID contained in both AHRS and RACF as of January 3, 2002, the date of the last reconciliation before audit field work was completed. After researching GUARD requests between those time periods we did not observe any PEUS004 related activity. In addition, the PEUS004 ID was determined to be valid RACF ID at the time of the final audit report.

Concur - HCUS030 RACF ID. The ID was deleted in January 2003.

C. Concur – Completed September, 2002. A monthly production report was implemented in September, 2002 that lists all AHRS users that have separated, transferred to another agency or department, or had a name change in the past 30 days. On a monthly basis each individual on the report is researched and appropriate changes are made to the AHRS security tables.

10. Dialog Between Human Resources, Auditor-Controller, and Information Systems

In a business process as complex as the County's payroll processing, it is critical to communicate regulatory pronouncements, contractual negotiations, and management policy.

Observation

We saw evidence of substantial interaction among staff involved in payroll and benefits processing. We congratulate the County on its ability to organize itself in a manner to facilitate orderly transaction processing. We have no recommendation on this point.

Management Response

County of Orange **MEMO**

March 11, 2003

TO: Peter Hughes, Director
Internal Audit

SUBJECT: Response to Internal Audit's Risk Assessment for CAPS Payroll Application

We have reviewed the draft report prepared by the Internal Audit Department covering its review of the non-monetary, monetary, and infrastructure risks within the payroll application. The audit report includes activities performed by Auditor-Controller, CEO-Human Resources and CEO-Information Technology staff. The attachment responds to recommendations made in the assessment.

Please call Mahesh Patel at (714) 834-3895 if you have any questions concerning our response.

David E. Sundstrom Auditor-Controller	Jan Walden Assistant CEO Human Resources	Daniel Hatton Assistant CEO Information & Technology

Attachment

cc: Eli Littner, Deputy Director, Internal Audit
Gary Burton, Assistant CEO, Finance and Budget
John Nakane, Chief Assistant Auditor-Controller
Jim McConnell, Assistant Auditor-Controller, Central Operations
Shaun Skelly, Assistant Auditor-Controller, Agency Accounting
Larry Chanda, Manager, CAPS Administration
Mahesh Patel, Assistant Auditor-Controller, Information Technology
Jim Berch, Accounting Systems Manager, Auditor-Controller
Ray Stephens, Payroll Systems Lead, Auditor-Controller
John Wheeler, Information Systems Manager, CEO-IT
Susan Paul, Employee Relations, CEO-HR
Marguerite Adams, Corporate HR Services,CEO-HR
Scott Sanders, Sr. Systems Analyst, CEO-HR
Phil Paker, ACS State and Local Solutions

Management Response Continued

1. Application Recovery Plan Inadequate For CAPS And CAPS Payroll

Recommendation

The County needs to enhance its application recovery plan and evaluate its risks from a significant CAPS outage. It should also be pointed out that the application recovery plan only addresses the mainframe environment. Restoring communications, obtaining access to system documentation at the Civic Center facility, and agency/department records needed to process CAPS payroll also need to be addressed in a comprehensive recovery plan.

Response

Partially Concur - It is correct that the County does not have an identified backup data center – or "Hot Site". We have investigated this option and believe that the costs are too great and cannot be justified given the level of risk and the current budget situation. However, we do believe that it is an important element of disaster recovery.

To address this issue we will explore possible lower cost options such as, a backup site provided by our major outsourcer ACS or a partnership with other California counties to provide mutual backup. To be complete by June, 2004.

It is correct that daily backups are stored on-site. However, weekly data center backups are stored off-site. These back-ups are sufficient to restore and run the CAPS system. The Data Center has a documented disaster recovery plan to restore the system from these backups at our site. The County considers that potentially losing several days of work is an acceptable business risk. We do not concur with this part of the recommendation.

The Auditor-Controller has developed a plan that addresses generation of payroll checks should a disaster occur.. It calls for creating a standalone process using information from the prior payroll to create either hardcopy checks or electronic payments. This process will be developed and tested as part of the CAPS upgrade project.

3. System Access To Production Datasets Bypassing Application Control

Recommendations

We recommend the local security administrators for CAPS complete their assessment for ALTER access to the Virtual Time Sheet datasets. Unless it is found that the application architecture requires this level of access, it should be removed.

We recommend that access privileges to production datasets be evaluated to determine if access is appropriate for functional analysts. We anticipate that the CAPS Upgrade will help to address this issue because it is table-driven by design allowing tables to be updated through application processes rather than system access.

We recommend that MMFINREC access group be reviewed to ensure that all users within the group require UPDATE access.

Response

Concur – Completed January, 2003. All VTI timesheet datasets have been converted from ALTER to UPDATE for agencies and department personnel.

Concur – Access to production datasets will be reviewed for appropriateness during the upgrade project. Estimated completion 2nd quarter, 2005.

Management Response Continued

Concur – Dataset UPDATE access for the MMFINREC access group will reviewed for appropriateness and exceptions corrected. Estimated completion 2nd quarter, 2003.

4. 28 User Names Have Application Access To *ALL Payroll Tables

Recommendation

We recommend the AC Local Security Administrator determine what, if any, security event reporting could be implemented. We also suggest security monitoring be a defined task within the CAPS Upgrade project that is just beginning.

Response

Concur – Critical Reference Tables in the Human Resources system have been logged, and reported to functional administrators on a daily basis, since the system's inception. The SLOG feature will be evaluated for usefulness in monitoring security events and deployed if found to enhance security beyond what is available from RACF. Estimated completion of SLOG evaluation 2nd quarter, 2003.

5. Premium Pay Input Is Decentralized And Prone To Error

Recommendation

Since premium pay has a contractual basis, we would recommend that Human Resources conduct a study of all premium pay to ensure conformance with the MOU. We further recommend that the CAPS Upgrade project address this issue as an opportunity to improve control and streamline workflow when establishing or changing an employee's status.

Response

Concur - Starting in approximately late Fall 2002 CEO HR Records began to audit premium pay that includes ensuring any errors found being corrected. This along with reports that Departments have to help them identify/correct any errors plus an online procedures manual (in development) will provide resolution to the issues noted relative to premium pay input being decentralized and prone to error. Also there is one bi-lingual rate code (BL) for which multiple rates are possible, which makes auditing of this code more difficult. We are looking into establishing a unique bi-lingual code for each unique rate which should thereby make auditing this function easier.

6. Basis For Computing Unemployment Reserves

Recommendation

We recommend that the experience and rate assumptions used by the County to determine its unemployment reserve be reviewed and validated as accurate.

Response

Do not Concur - The current unemployment premium rate of .0015 is developed to fund the annual unemployment claims paid as a direct reimburser through the State Employment Development Department for unemployment benefits. It is not a reserve, nor does it have any portion of the rate designed to fund a reserve. Current retained earnings are sufficient to fund a reserve necessary to pay future base period claims.

Projected claims are determined using analysis of average quarterly claims costs over the last 12 months period, adjusted to reflect 1) changes in unemployment benefits or length of claim as mandated by legislation and 2) increases or decreases in quarterly claims cost due to changes in the overall labor market due to the economy and/or changes in the County turnover rate.

Recent changes in the legislation increasing the weekly benefit amount and length of claim were factored into the current rate however global economic conditions and reductions in County workforce due to the budget crisis could impact future claims. As unemployment claims increase either due to increased length of claim or due to an increase in the number of claimants, the current rate of .0015 may need to be adjusted.

However as pointed out in the internal audit observation above, at the current time, the existing method of self funding as a direct reimburser is much less costly than participating in the State fund as a tax rated employer. In fact, the County currently contracts for administration of unemployment claims management with Gates McDonald through a consortium of other California Counties known as the County Personnel Administrator Association of California, CPAAC. Participation with the CPAAC consortium provides the advantages of combined efforts on legislative action, pursuit of recovery of state mandated expenditures, sharing of consortium data and having input into the state on administrative regulations.

Also, as a clarification, our records show that the estimated salary of an average County employee is approximately $50,000 rather than $35,000.

7. Published Title Table Appears Out Of Date

Recommendation

We recommend this finding be researched and the Title Schematic be updated on the web site, if necessary. We also suggest that the 91 staff be reviewed to ensure they are authorized for rates above the table maximums.

Response

Do not Concur - Although noted by ISecurePrivacy that their findings included almost 2000 staff with a title not found in a title table dated 8-2-2002 we believe that ISecurePrivacy may have been provided with a title schematic dated 8-2-02 which specifically applies to the County titles and not the full titles that are in AHRS which includes other entities such as the Courts and special districts.

8. Medicare Differences And Non-Payments

Recommendation

We believe, based on representations from County staff, that appropriate action is being taken to resolve these employee Medicare issues.

Response

Concur -The Auditor's Office/Central Payroll Section is currently reviewing our listing of potential Medicare discrepancies, which will result in corrective action being taken to ensure that eligible employees are being subject to the Medicare tax. Additionally, action will be initiated requiring that a biweekly report be generated

Management Response Continued

for the purpose of identifying potential Medicare issues in a timely manner. Estimated completion is 4th Quarter 2003.

9. Application Security Profiles Are Deployed

Recommendation

We believe there are opportunities for creating additional efficiencies within the application security group by evaluating the need for so many profiles. We recognize this is not a trivial task, and suggest it be accomplished during the CAPS Upgrade rather than undertaken within the current environment.

We recommend the PEUS004 and HCUS030 user names be researched and deleted as appropriate.

We recommend implementation of a security capability to notify local security administrators in a timely manner when a staff member transfers or terminates.

Response

Concur – A limitation within the Advantage 2.x product will not allow granting of multiple profiles to an individual. This limitation requires the need to create unique profiles for some users who are authorized for several access types (e.g., budget and HR). It is our understanding that the Advantage 3.x product allows the assignment of multiple profiles to an individual which should alleviate the need to have unique profiles. This issue will be addressed in the upgrade project.

Partially Concur – PEUS004 RACF ID. The User ID's contained in the AHRS security tables are periodically reconciled to RACF and discrepancies resolved. PEUS004 was a valid ID contained in both AHRS and RACF as of January 3, 2002, the date of the last reconciliation before audit field work was completed. After researching GUARD requests between those time periods we did not observe any PEUS004 related activity. In addition, the PEUS004 ID was determined to be valid RACF ID at the time of the final audit report.

Concur - HCUS030 RACF ID. The ID was deleted in January 2003.

Concur – Completed September, 2002. A monthly production report was implemented in September, 2002 that lists all AHRS users that have separated, transferred to another agency or department, or had a name change in the past 30 days. On a monthly basis each individual on the report is researched and appropriate changes are made to the AHRS security tables.

Recommendation No. 8: We recommend the Clerk-Recorder amend their System Development Guidelines to include all areas of the system development lifecycle including project planning, development, and testing.

Clerk-Recorder Response:
Concur and implemented.

9. I/S Policies and Procedures

Policies and procedures for the Clerk-Recorder's I/S Division did not address physical security issues and the software/hardware acquisition life cycle.

The Clerk-Recorder operates a data center that houses application servers. The Clerk-Recorder's current security policy was only sent to managers and supervisors, and does not address physical security issues such as who is allowed access to the data center, how to manage the CCD surveillance system, and how to monitor environmental controls. Additionally, there are no documented procedures for the purchase, maintenance, and disposition of hardware and software.

Failure to properly document policies and procedures could result in unauthorized access to department information assets and inefficient use of I/T infrastructure.

Recommendation No. 9A: We recommend the Clerk-Recorder amend their Security Policy to include physical security and distribute it to all personnel.

Clerk-Recorder Response:
Concur and implemented.

Recommendation No. 9B: We recommend the Clerk-Recorder document policies and procedures for the purchase, maintenance, and disposition of hardware and software.

Clerk-Recorder Response:
Concur, with implementation scheduled for June 1, 2003.

10. Automatic Workstation Lock-Out

Workstations are not automatically set to lockout the user when no activity occurs over a set amount of time. Failure to enable automatic workstation lockout by the operating system could result in unauthorized access to department information resources.