INFORMATIONAL DOCUMENT FOR AUDIT COMMITTEE

Completed Closed Audits

Dante Robinson, Chief of Internal Affairs

CDI Operational Review PAO 672

Objective/Scope

PWC conducted a review with Internal Audit oversight of State Fund's processes, controls and documentation, which were implemented in response to California Department of Insurance Operational review performed in 2007 with follow-up reviews conducted in 2008 and 2010 which had 145 findings. The period under review extended from January 1, 2011 to July 31, 2012.

Methodology

- Conducted interviews with individuals charged with responsibility over the original CDI findings.
- Assessed the design and operating effectiveness of processes and controls related to the CDI findings.
- Performed testing over the operating effectiveness of controls implemented to remediate the CDI findings.

Findings

PWC determined that 104 of the findings had been remediated and 41 findings were identified as un-remediated**.** Of the 41 un-remediated findings 13 were rated as high risks. The un-remediated high risk issues were:

1. Increase the Size of State Fund Board, Review Director Qualifications, Training Curriculum, Compensation and Meeting Frequency
2. Segregation of Duties Issues
3. Business Recovery Plans Outdated
4. User Administration Procedures Not Formalized
5. Oracle Audit Logs Not Consistently Reviewed
6. Data Tape Encryption Not Performed

7. Performance and Capacity Monitoring Not Performed
8. Data Center Physical Access Activity Not Reviewed
9. Home Office Help Desk and Support Not Monitored
10. All Claims Processing Centers: Late Payment Penalties Increase
11. Burbank Claims Processing Center: Ensure Access Controls to Archive Room is Restricted
12. Significant Contracts Signed by Inappropriate Personnel
13. Procedures Should be Established to Safeguard State Fund Assets and Information

Remediation

1. Board member has completed the training. Learning and Development and Board Liaison will have a report provided on required training prior to completion deadline and will inform any Board member of the deadline.
2. Reviewing task and management ownership, engaging Human Resources and business units to develop standards, and identifying data owners for each application and working to bring clarity to all roles and responsibilities associated with each step in the approval process.
3. ESEC will send security subject matter expert to each of the offices and storage facilities to perform assessment of physical controls. IT will be establishing an ongoing testing program including periodic testing of disaster recovery plans.
4. Reviewing the tasks and management ownership, engaging Human Resources and business units to develop standards for responsiveness, and develop account management standards, that may include the recommended topics.
5. IT will perform a review of application security log configurations starting with the highest risk system and develop a plan to implement enhancement to logging controls.
6. A project effort has been put together to implement the required backup data replication to Riverside.
7. A new Network Operations and Controls Center (NOCC) team will be established as part of the new IT reorganization and the necessary monitoring tools will be implemented in parallel with that effort.
8. Required policies and procedures will be developed, and efforts have been taken to address access to data center floor. Sign-on list has been implemented and Chief Technology Officer will work with ESEC to put together a monthly review and audit process against the access list.
9. IT will develop the necessary SLA and process as part of the IT service improvement effort.
10. Short term solution is to use the Talent Resource Program and a vendor. Long term solution hiring of replacement staff and improving efficiencies through better business processes and technological solutions.
11. Employees not currently needing access will begin stripping and scanning of files in the warehouse and will therefore need access.

12. Oracle profile for these employees has been updated and access restricted. Enterprise Procurement will conduct periodic reviews to ensure access limited to only appropriate personnel.
13. Human Resources Operations has taken responsibility for certifying that the separation process is completed for each employee, which includes ensuring the Expert Support Program (ESP) process has closed.

Proprietary: No

Corporate Physical Access Security PAO 667

Objective/Scope

Assess Real Estate Management's execution of their responsibilities; compliance with Corporate Guidelines, policies, directives, and procedures. Gain an understanding of how physical access procedures are conducted throughout the organization. Identify opportunities to enhance the efficiency and to address gaps in the current physical access security procedures and practices for the period January 1, 2011 through January 3, 2012.

Methodology

- Interviewed 10 property managers for information about physical access security procedures and practices.
- Reviewed network video surveillance devices to assess the effectiveness of the security monitoring system.
- Surveyed 135 employees to obtain information regarding their knowledge and awareness about physical access procedures.
- Conducted interior and exterior perimeter inspections after hours.
- Reconciled REM Cardholders Access lists with Human Resources Separation List for year 2011.

Findings

1. Chatsworth – Personal Identifiable Information and HIPPA security.
2. Stockton Regional Office – Excess Access for Security Guards.
3. Stockton Regional Office – Incorrect code label assigned to an electrical room.
4. Vacaville Regional Office – Incorrect access levels provided.
5. Vacaville Regional Office – No backup power source.
6. Pleasanton Regional Office – System detection security.
7. Pleasanton Regional Office – Deactivated dates data integrity.
8. All Offices – Supervisor submission of separation checklist and staffing.

9. All Offices – Visible employee ID badges.
10. Rohnert Park State Contracts – Not part of the Lenel Security System.
11. All Offices – Unsecured desktops and laptops.

Remediation

1. Test all external doors after hours and have any problem doors repaired. Procedure will be implemented that will instruct and require janitorial staff/company to inform Property Managers when someone tries to gain access or does gain access to the building after hours.
2. Write and implement a procedure for security personnel physical access, complete procedure, provide to staff, and validate access changes to security guard access that is not in compliance.
3. Check that only appropriate personnel have access to main electrical rooms, revalidate electrical, fire panel and similar type building operations rooms are properly labeled in Lenel Access. Remove non REM/emergency responders from these rooms.
4. ESEC lab access to be reviewed at same frequency as Data Center. Write procedure card keys must be used at ALL times to enter any room. Procedure will be distributed to all REM employees.
5. Lenel readers have a battery in them so there is back up to Lenel system and readers in event of main power failure.
6. Look into whether an email or audible alarm can be done with Lenel System, and if alarm is possible implement in 2013.
7. Inform and remind all Property Management staff NOT to back date the time they actually deactivated someone's badge.
8. Review the process again and make improvements to it, and set up a back-up process to ensure completed within 48 hours.
9. There is no consequence when someone fails to wear badge, REM sends out reminders quarterly to wear badges conspicuously and to not let anyone tailgate behind them. REM will install signage in all locations.
10. Rohnert Park will be integrated with Santa Rosa Regional Office, which is on the Lenel Security System.
11. Developing physical inspections survey, which includes privacy and information security-related issues. Surveys will be disseminated to all departments with instructions to complete every quarter. Managers will be required to certify completion of inspection. Privacy and security violations will be subject to progressive discipline by Human Resources.

Proprietary: No

2012 Underwriting Audit PAO 680

Objective/Scope

Walk-through the Underwriting processes to assess the design of operational, financial, and monitoring controls and processes currently in place within the organization. Specific audit coverage included process walkthroughs, creation of process flow charts, and detailed testing in areas of identified risk.

Methodology

- Review of underwriting files to verify inclusion of required submission documents, including review for X-mod, class codes, application of discounts, and schedule of debits and credits.
- Approval of high risk class codes and large dollar policies.
- Review of procedures associated with multi-state policies, 304 billings, straight through renewal process, adding / removing policy endorsement, and identifying and reporting possible premium fraud.
- Review of field office operations.
- IT baseline of Underwriting three tier rating system and review of the Single Quoting Engine (SQE).
- Validity and monitoring of performance metrics.

Findings

1. Tracking of Premium Receivable - Claims can potentially be processed and paid prior to receipt of policy premium.
2. Skeleton and Temporary Policies - Claims can potentially be processed and paid prior to verifying an active policy exists.
3. Tracking of Policy Changes - A complete population of material policy changes is not maintained.
4. Lack of Approval Verification – PowerComp Quote approvals from the previous quoting engine (PowerComp) were not available for testing.
5. Lack of Approval Verification SQE - Appropriate approval for large dollar policies is not always evidenced and retained.
6. WCIRB Inspection Reports - Policies are not written in accordance with existing state records (i.e., name of insured, explanation of gaps in policy coverage, etc.)
7. Consolidated Servicing Information - Noted that the Consolidated Servicing Information (CSI) module assigns tasks to (a) an Underwriter and (b) a regional queue based on the policy's attributes. However, no single definitive source exists for associating an Underwriter to a unit or Regional office. As a result, discrepancies may occur if the assigned Underwriter does not match the unit or regional office to which the task was assigned.

8. Systematic Update of the Broker - The Broker of Record (BOR) desk does not have access to update the broker of record within Work Management.
9. 304 Billing - 304 billing may be inaccurate and/or lack proper supporting documentation. Noted the following testing exceptions through review of in-force policies related to 304 billing
10. Endorsements Requiring Approval - Evidence of approval for endorsements is not always maintained.

Remediation

1. Management will work with Corporate Claims to put in place a new process related to policy and procedure PROPS 20-00-002 and 20-00-006 and link them to the Corporate Claims Procedures. Management will also be re-examining policy and procedure PROP 20-00-824 Rescission of Policy Contract - C7 and C8 to determine if the appropriate procedures are in place to mitigate risk of loss.
2. Management will work with Corporate Claims to put in place a new process related to policy and procedure PROPS 20-00-002 and 20-00-006 and link them to the Corporate Claims Procedures. Management will also be re-examining policy and procedure PROP 20-00-824 Rescission of Policy Contract - C7 and C8 to determine if the appropriate procedures are in place to mitigate risk of loss. Additionally, Management is examining the formation of skeleton and temporary policies and will make recommendations to eliminate policies that do not originate in RAQ or SQE.
3. Management will send an Underwriting update memo to remind Underwriters to appropriately enter items in the Activity Log for any updates on a policy and/or discussion with a broker or policyholder. Additionally, during November 2012, Management will select a sample of policies and perform a self audit of the activity log noted for completeness and accuracy.
4. Management has initiated discussions with IT and the CIO to determine the best method for recovering access to the legacy system (PowerComp) audit trail. Management expects to have a detailed response and action plan from IT by mid October 2012.
5. Large accounts of $250,000-$499,999 are submitted to Corporate Underwriting for review and approval. The Corporate Underwriting Consultant has the complete ownership, authority and responsibility of reviewing and approving the ultimate Schedule Rating points assigned. Management will reinforce the expectation and ensure that evidence of review by the Senior Underwriting Consultant or the Corporate Underwriting Supervisor is maintained on SFO. Accounts with less than five point deviation may also be reviewed by the Senior Underwriter or Supervisor. A database for large accounts is kept and monitored quarterly for policies bound on the mainframe to assure compliance.
6. 73% of WCIRB queries are resolved by the Policy Analyst within 30-days. Management is currently researching WCIRB queries to determine the root cause of common types of queries, such as lapses in coverage and ownership questions. A root cause analysis will allow Management to improve operational

efficiency by communicating trends, identifying training needs, and developing ways to automate distribution and tracking of queries. Additionally, State Fund is undergoing a system integration project to streamline and electronically match Bureau IDs and State Fund policy IDs.

7. Management is aware of these issues and it is working to mitigate these system deficiencies. CSI (the assignment engine) does not currently meet the needs of State Fund. Currently, State Fund is working on an improved assignment engine that can handle these functions.
8. Management is in the process of submitting a project proposal/change request for functionality that was not included in the initial release (i.e., BOR desk access to make updates to the broker of record). In the interim, the BOR desk only needs to contact the underwriter for the broker of record changes on renewals. New Business requires the underwriter to close the submission out if updates are required to the broker of record.
9. 304 billing plans are initiated and calculated by Underwriting. Management will review the current review procedure in place for 304 billing plans to ensure proper controls are in place and delineate who is responsible for the accuracy and calculation method of the bill.
10. Endorsements can be added after the policy incepts and many of the approval authorities were disbursed to the regional offices a few years ago. When an endorsement is added after the policy incepts and approvals are needed, the approvals should be granted in SFO and tracked in the Activity Log. Management will review the current procedures in place and ensure proper approvals are maintained for endorsement added after policy inception.

Proprietary: No

2012 Marketing Audit PAO 665

Objective/Scope

Walk-through the Marketing processes to assess the design of operational, financial, and monitoring controls and processes currently in place within the organization. Specific audit coverage included process walkthroughs, creation of process flow charts, and detailed testing in areas of identified risk.

Methodology

Broker Maintenance

- Broker file review to verify active license, proof of sufficient E&O insurance coverage, and a signed broker agreement

- Review the monitoring control for license and insurance
- Confirm broker classification between standard and preferred is approved

Commissions

- Review the accuracy of system rates, commission calculations, and disbursements
- Confirm commissions are approved before being processed for payment
- Review controls over returned checks and reimbursements for negative commissions

Performance Metrics

- Evaluate the validity of department and broker metrics

Findings

1. Quarterly Monitoring of Broker Licenses and Insurance per established MAR controls, Contract Management should be performing quarterly monitoring procedures to ensure broker licenses are current and E&O insurance is in place for all brokers. These procedures have not been performed since October 2011.
2. Timeliness of Receiving Annual Broker Contracts - Annual broker renewal contacts are not all received by the December 31 due date.
3. Proper Handling of Returned Monthly Commission Checks
4. Broker commission checks being returned in the mail are not being adequately tracked and monitored.

Remediation

1. Contract Management is in the process of confirming broker license and obtaining proof of insurance. As of 9/27/12, 80 licenses remain to be verified and 2,856 insurance certificates need to be obtained. This process will be completed by 10/31/12. Contract Management will ensure that the quarterly review is performed on a go forward basis.
2. Contract Management will trend the timeliness of obtaining renewal contracts beginning with 2013 renewals. Marketing will create and distribute a broker contract renewal timeline for 2013. Currently an action plan exists for processing of contracts. Going forward, a more specific timeline will be established and followed.
3. Contract Management will ensure that the data captured in the log is consistent and will review the log monthly beginning in October 2012. All brokers will be signed up for EFT during the 4th quarter of 2012. Procedures for the return of monthly commission checks process have been completed.

Proprietary: No