**PNW - Higher Education Internal Audit Conference**

**Aug 10 – 12, 2011**

**UBC Speaking Notes:**

1. **Fraud uncovered using ACL**
   * Match of employee/vendor name or address or postal code
     1. Joined Vendor table (from A/P) and Employee table (from Payroll) to identify vendors with the same addresses and postal codes as the employee addresses and postal codes.
     2. Because there was a huge number of duplicates and false positives in our data, we joined the Vendor and Payroll tables to summaries of vendor payments over a period of time.
     3. We further filtered to eliminate valid employee and student vendors, invalid of non-Canadian addresses, and employees without payroll in the scope period.
     4. We then sorted in descending order by the gross amount paid to the individual vendors in the scope period.
     5. Then used judgmental sampling to select vendors that appeared to be consulting firms or general businesses with larger gross amounts paid.
     6. We judgmentally selected one requisition from each of the vendors chosen for audit testing.
   * Discovery of potential ‘fraud’
     1. The invoice for 1 of the requisitions looked unusual so we pulled requisitions for additional payments to the same vendor.
     2. We discovered over $400K in payments to the same vendor, authorized by the employee.
     3. Interviewed employee. He has been terminated.
     4. Reported to RCMP & insurance. Under investigation by RCMP.
2. **Other ACL tests – fraud detection**
   * *Same Bank Details, Different Vendor Code*
     1. This test was performed by identifying and extracting vendors where the registered bank details were identical.
     2. For each of the matches we pulled vendor payments during the scope period.
     3. The test confirmed no external vendors with duplicate bank accounts. However, we have very few vendors set up with EFT (electronic funds transfer) so this test was somewhat limited at this point).
     4. All matching vendors were employees.
        1. We assumed all matches with the same last name were family members.
        2. Checked addresses on HR system. For those employees with same address, assumed they were couples.
        3. Further work done for matches with different names and addresses.
           1. A few exceptions found but with valid explanations i.e. medical clinic – doctors depositing their salaries to shared clinic account.
   * *Consulting Payments in Research Grants for Matched Vendor and Employee Addresses*
     1. Refined the address match test used to detect the large fraud. Focused on consulting payments in research grants.
     2. A list of vendors with consultancy fee payments was filtered by joining the vendor/employee address match test results.
     3. The highest risk payments were to those with signing authority on the account where the payment was charged. Therefore, we further filtered the test results by joining the results to employees with signing authority. (PG Signing authority table records all current & historic employees with PG level signing authority.)
     4. The results were reviewed:
        1. We pulled vendor payments and reviewed backup to check if the authorizing person owned or was associated with the vendor.
        2. Checked for false positives
           1. Reviewed employee details in the HR system to ensure that there was an address match
           2. Reviewed signing authority to ensure employee had signing authority
        3. Identified payments for further review – potential fraud or conflicts of interest/commitment.