Countering Fraud Risk

Managing Business Integrity and Internal Control to Ensure Compliance: A Bank Case Study

Date & Time : 27 August 2014; 10.45am-16.00 pm

Speaker Profile

PAIRAT SRIVILAIRIT, CIA, CISA, CISSP, CFE, is Head of Governance Office of TISCO Financial Group, PLC. and enables organization in the use of Computer-Assisted Audit Tools and Techniques (CAATS) technology to address weakness in business operation and control, and detect frauds. He is associated with finance and banking industry for over 20 years with rich experiences in the area of management consulting, planning, research, investment, operation and audit, and is a known lecturer on operational auditing and fraud examination courses. He can be contacted at *pairat@tisco.co.th*

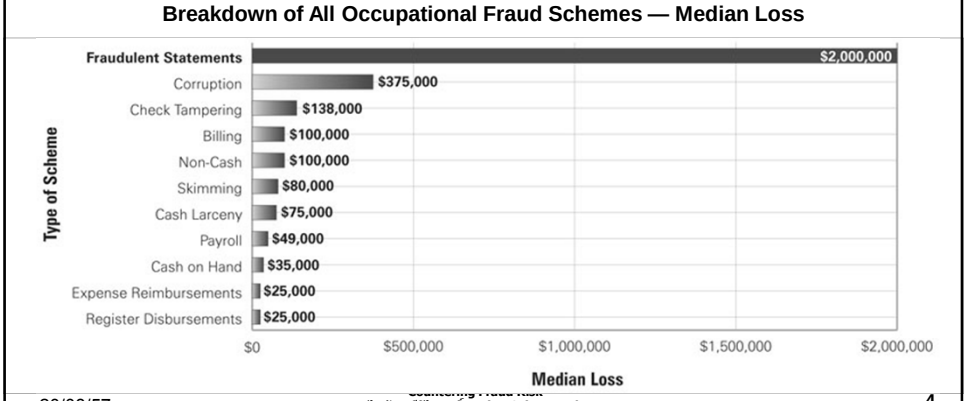
Outline

Countering Fraud Risk – Managing Business Integrity and Internal Control to Ensure Compliance: A Bank Case Study

- Most common fraud – understanding how it is committed and detected
- Key indicator of fraud – symptom of fraud and trend in banking industry
- Insider threat – internal computer fraud and misuse / application control
- Fraud prevention checklist - Internal control systems to mitigate risk of fraud and ensure compliance

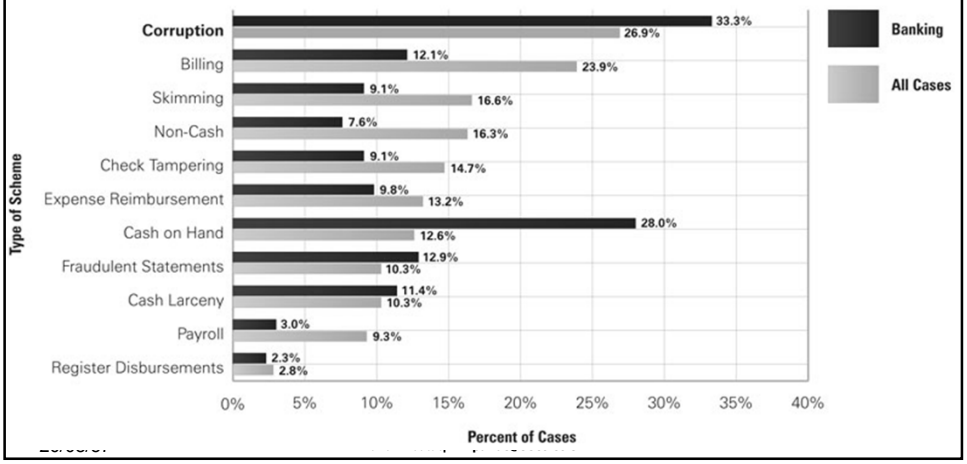
How Fraud is Committed

- Asset misappropriations were most common but low loss. Fraudulent statements were least common with highest loss.



Bank Most Common Fraud

- Greatest percentage (15%) of fraud occurred in banking and financial services sector.



ตัวอย่างทุจริตในธนาคาร

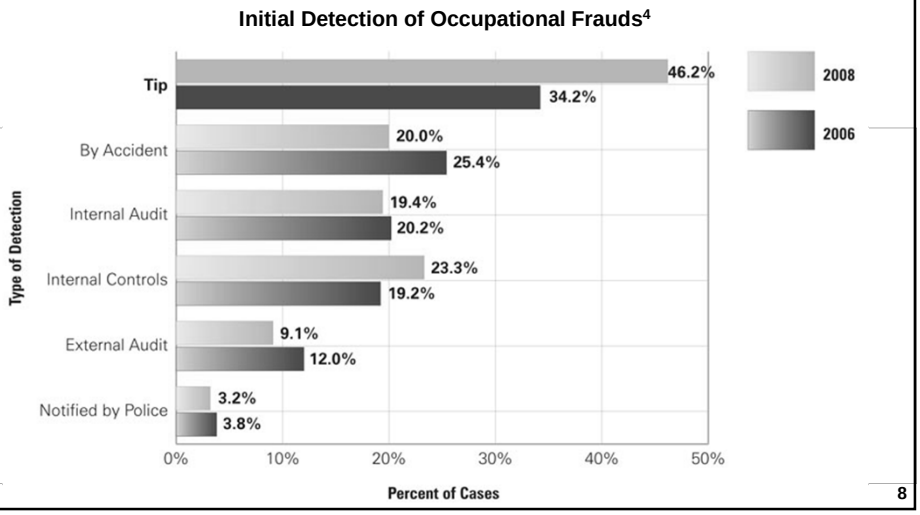
- การทุจริตโดยพนักงานธนาคาร
  - พนักงาน ขโมยเงินสด ของสาขาไปใช้ประโยชน์ส่วนตน
  - พนักงานสาขา ปลอมลายมือชื่อ ลูกค้าที่บัญชีไม่เคลื่อนไหวนาน หรือ ยักยอกบัตร และรหัส ATM ที่ลูกค้ายังไม่มารับไปและถอนเงินไปใช้ส่วนตัว
  - พนักงานสินเชื่อรับชำระค่างวด ค่าธรรมเนียม หรือค่าประกันจากลูกค้า และ ไม่นำส่งธนาคาร
  - พนักงานบรรจุเงินสดในเครื่อง ATM ไม่ครบตามที่แจ้งไว้ หรือ ขโมยเงิน ที่เครื่อง Reject ออก
  - พนักงานสินเชื่อหรือผู้บริหารรู้เห็นกับลูกค้า ประเมินมูลค่าหลักประกันสูง กว่าความเป็นจริง.

ตัวอย่างทุจริตในธนาคาร

- การทุจริตโดยลูกค้าและบุคคลภายนอก
  - ปลอมเว็บไซท์ของธนาคาร เพื่อหลอกลวงข้อมูลจากลูกค้าไปใช้ทำทุจริต (Phishing)
  - ใช้การทำ ธุรกรรมที่ซับซ้อน กับธนาคารเพื่อปกปิดแหล่งที่มาของเงิน (Money laundering)
  - เสนอ ผลประโยชน์ที่สูง หรืออ้างตัวเป็นเจ้าหน้าที่ทางการเพื่อหลอกลวงข้อมูลหรือเงินจากบัญชีลูกค้า
  - ปลอม เอกสารแสดงตนและหลักฐานการเงิน เพื่อกู้ยืมจากธนาคารโดยเจตนาไม่ชำระคืน
  - ติด อุปกรณ์อ่านแถบแม่เหล็กและกล้องวิดีโอ ที่ตู้ ATM เพื่อทำสำเนาบัตรและเบิกเงินจากบัญชีลูกค้า (Skimming).

How Fraud is Detected

- It takes 24 months on average to catch employee fraud



Key Indicators of Fraud

- Tips / Complaints
- Missing / Alteration of documents
- Duplicate / Unreasonable expenses or reimbursements
- Failure of certain employees to take vacations
- Failure to follow up on past-due receivables
- Unusual write-offs of receivables
- Employees on the payroll not sign up for benefits
- Excessive purchase of products or services
- Common phone numbers / addresses of payees or customers

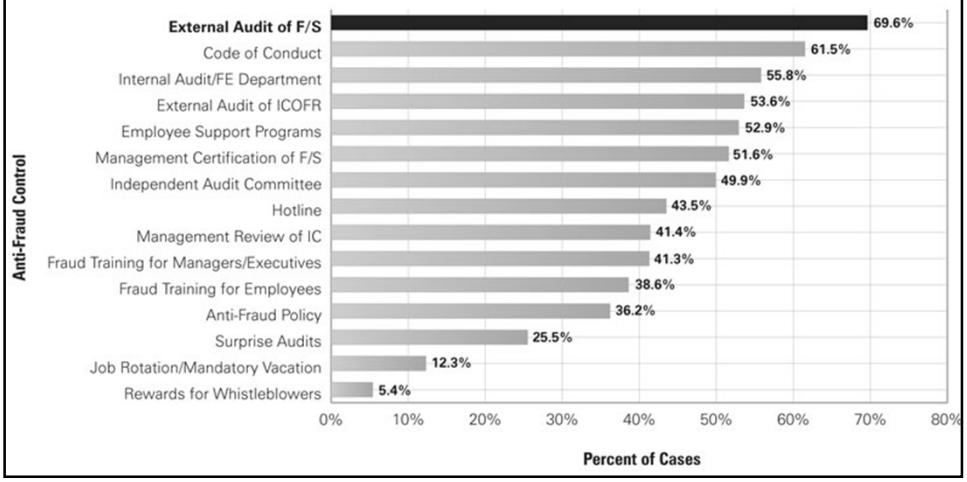
Key Indicators of Fraud

(Continued)

- Cash shortages / overages
- Stale items on bank reconciliations
- Unexplained adjustments / Journal entries
- Unusual financial statement relationships i.e.
  - Increased revenue vs. decreased receivable
  - Increased revenue vs. decreased inventory purchase
  - Increased inventory vs. decreased purchase or A/P
- Significant increases or decreases in account balances
- Significant changes in liquidity, leverage, profitability or turnover ratios

Limiting Fraud Losses

- Surprise audit and job rotation are still overlooked by many organizations.



Limiting Fraud Losses

- Surprise audit, job rotation, and anonymous reporting showed the greatest impact on fraud losses.

Median Loss Based on Presence of Anti-fraud Controls				
Control	**% of Cases Implemented**	**Yes**	**No**	**% Reduction**
Surprise Audits	25.5%	$70,000	$207,000	66.2%
Job Rotation / Mandatory Vacation	12.3%	$64,000	$164,000	61.0%
Hotline	43.5%	$100,000	$250,000	60.0%
Employee Support Programs	52.9%	$110,000	$250,000	56.0%
Fraud Training for Managers / Executives	41.3%	$100,000	$227,000	55.9%
Internal Audit / FE Department	55.8%	$118,000	$250,000	52.8%
Fraud Training for Employees	38.6%	$100,000	$208,000	51.9%
Anti-Fraud Policy	36.2%	$100,000	$197,000	49.2%
External Audit of ICOFR	53.6%	$121,000	$232,000	47.8%
Code of Conduct	61.5%	$126,000	$232,000	45.7%
Management Review of IC	41.4%	$110,000	$200,000	45.0%

12

Bank Case Symptoms

- Supervisory override, unusually large transactions or with no apparent business purpose
- Journal voucher contain only one signature, containing incorrect information, fund transfer between different customers' accounts
- Deposit slip with missing information, depositor names incomplete or not match with passbook or acct name.
- Frequent, large deposit/withdrawal in Executive account
- Deposits and withdrawals on same account on same day or in a short period of time
- Bank checks used to transfer between accounts / checks with altered date.

Symptoms ... More

- Purported customer signature on withdrawal voucher and checks
- Large negative balances in slush accts or customer accts
- Deposit slip of customer funds between accts of different customers
- Deposits of customer check where cash was received back
- CDs closed prematurely with proceeds put into low interest account, sometimes with penalty
- Customer not presented when account was opened, closed or transacted
- Mailing of customer statement to Executive address

Bank Fraud Trend

- Fraud financial cost may be three or more times the value of loss amount
- Fraud is not static. It evolves with each new measures implemented
- New opportunities for employee fraud are emerging
- Criminals thwart rules-based systems
- “Silo” mentality weakens fraud detection
- Top management are moving toward an enterprise focus on anti-fraud systems
- Regulatory expectations are increasing
- Solutions require commitment, investment, and talent

Insider Threat

- “Deliberate misuse by those who are authorized to use computer and networks.”
- Insiders include employees, contractors, consultants, temporary helper, personnel from third-party business partner, etc.

Facts about Insider Misuses

- Most were not technically sophisticated or complex
- Most were thought out and planned in advance
- Most were motivated by financial gain
- Most perpetrators of banking and finance incidents
  - Not hold technical position
  - Never engage in technical attack or hacking
  - Not necessarily perceived as problem employees
- Executed at workplace during normal business hours
- Detected by various channels and methods.

20/08/57

17

Misuse of Applications

Applications	Legitimate Use	Misuse
Client/Server	▪ Message exchange ▪ Connectivity to server ▪ Execution of tasks	▪ Unusual exchange to degrade performance ▪ Exceedingly connection (DOS) ▪ Execute privileged procedure
Mail Clients	▪ Send and receive e-mails	▪ Illegal content / remote attack / private use / overload network
Browsers / Multimedia player	▪ Browse Internet / play files ▪ View cached file and history	▪ View illegal content ▪ Display other users' viewed files and accesses
Programming Tools	▪ Develop program ▪ Display memory segment	▪ Create malware ▪ Access memory segment with sensitive information
General-purpose Applications	▪ Read / write ▪ Input strings	▪ Access temp file for sensitive information / modify temp file to change program flow ▪ Buffer overflow

18

Universal of Internal Computer Fraud

Computer Fraud

Billing Schemes
- Forged Endorsement
- Corruption & Price initiation
- Ghost Vendor
- Accomplice Vendor
- Quid Pro Quo & Barter Schemes
- Return & Voids
- Personal Purchase
- Passing of Payment of Invoices for Non-existing Suppliers

Data Capture
- Spyware & Key loggers

Fund Transfer
- Unauthorized Transfer of Funds

Errors
- Duplicate Payments
- Over Payments
- Payment to Erroneous Employees & Vendors
- Early Payments
- Missing or Bad Information
- Duplicate Information

Manipulation of Data Input
- Data Integrity Attack
- Falsification of Stock Record to Cover Theft of Stocks
- Data Suppression

Program Altering Schemes
- Changing Program and Data Ownership
- Setting Improper Parameter
- Use of Malware (e.g. Trojans)
- Alteration of Program and Data File

Information Privacy Risk
- Loss of Intellectual Property Through Fraud
- Transmission of Confidential Data (i.e. TCP/IP)
- Employee Downloading Hacker Tools For ID Theft Purpose
- Peer-to-peer Filing Sharing
- Employee Posting Confidential Company Information
- Employee Downloads & Nefarious Applications

Payroll Schemes
- Ghost Employee
- False Communication
- Worker's Compensation Scheme
- Falsified Wages

Check Tampering
- Forged Endorsement
- Skimming
- Forged Checks
- Write-off of Money Due to Company
- Alter Payee

Types of Application Controls

Application Controls

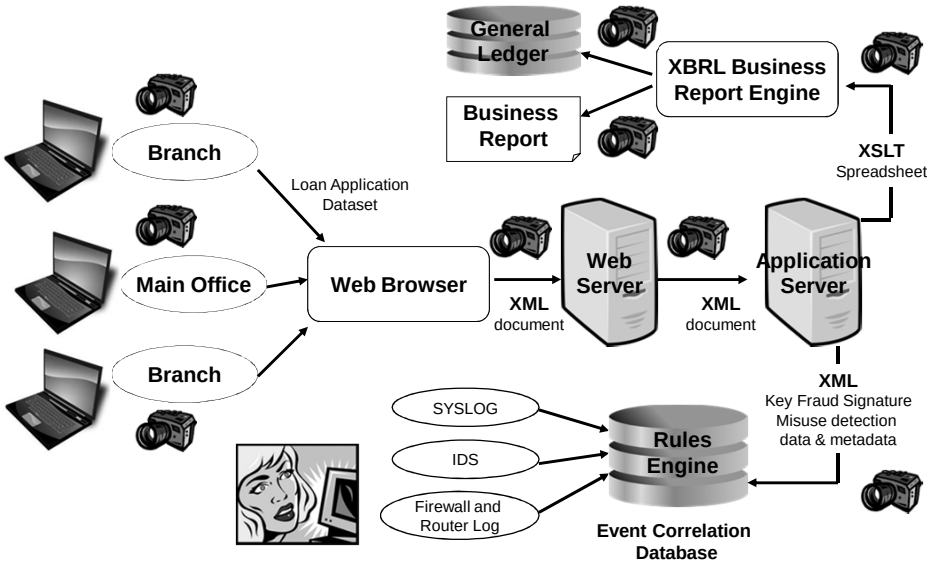
Access Controls
- Identification & Authentication
- Authorization
- Accountability
- Audit
- Physical Devices (i.e. biometric scan, metal locks, hidden path, digital signatures, encryption, social barriers, human and automated monitoring systems etc.),
- Permit or deny use of an object

Data Origination / Input Controls
- Check Integrity of Data entered Into Business Application
- Check whether sources from staff direct input, remote by business partner, or through web-enabled application
- Check if data is within specified parameter
- Ensure accuracy, completeness and timeliness of data during conversion from original sources into computer data or entry to computer application either manual, online input or batch.
- Ensure accuracy with optimum computerized validation and editing,
- Error handling procedure facilitate timely and accurate resubmission of all corrected data

Data Processing
- Ensure accuracy, completeness and timeliness of data during either Batch or real-time processing by application.
- Ensure data is accurately processed through the application
- No data is added, lost or altered during processing

Output Control
- Ensure integrity of output and the correct and timely distribution of output produced either in hardcopy, files to be used as input for other system, or information available for online viewing

Example of Detection System



Managing Insider Threat

- Strong authentication / biometric technologies
- Role-based access granted on a need-to-have basis
- Rotate job function / event log reading
- Place server and sensitive equipment in secured area
- Restrict physical access / lock / alarm test
- Wear badge / background check
- Default password / unused port / log-off on absence
- Encrypt sensitive data stored on user hard drives
- Store sensitive document in secured space
- Never issue password over unsecured channels

Aware of Warning Signs

- Rogue access point / wireless / remote
- Disgruntled employee
- A user accesses database or area of network they have never accessed before
- Download spike

Fraud Prevention Checklist

- Good internal control
- Employee fraud awareness training / hotline
- Analytical review / surprise fraud audits
- Review company contracts
- Perception of detection / management oversight
- Proactive fraud policy and program / prosecution
- Mandatory vacations / periodic job rotation
- Screen job applicants
- Information security review / limit access / audit trail
- Management climate / employee support program

Summary

Your roles in combating fraud

- Promote culture of honesty and high ethics
- Assess and mitigate the risk of fraud
- Ensure control adequacy and effectiveness
- Use data mining and statistical analysis tools
- Analyze financial statements reports
- Being alert on predication of fraud
- Ensure investigations are properly conducted
- Ensure proper follow-up actions are taken
- Develop your anti-fraud knowledge and skills

Q&A

PAIRAT SRIVILAIRIT
AEVP Head of Governance Office
TISCO Financial Group Public Company Limited
Mobile : +668 1903 1457
Office : +66 2633 7821
Email : pairat@tisco.co.th