คลินิกไอเอ ครั้งที่ 48
(ISACA 18th Quarterly Seminar)

ทุจริตจากภายในองค์กร

(Internal Fraud)

ณ ห้อง 303 ชั้น 3 ตลาดหลักทรัพย์แห่งประเทศไทย
ถนนรัชดาภิเษก
วันเสาร์ที่ 20 กุมภาพันธ์ พ.ศ. 2553 เวลา 9.00-12.00 น.

The Institute Of Internal Auditors Of Thailand

ตลาดหลักทรัพย์แห่งประเทศไทย
The Stock Exchange of Thailand

ISACA
ส่งเสริมธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ
Bangkok Chapter

About ISACA

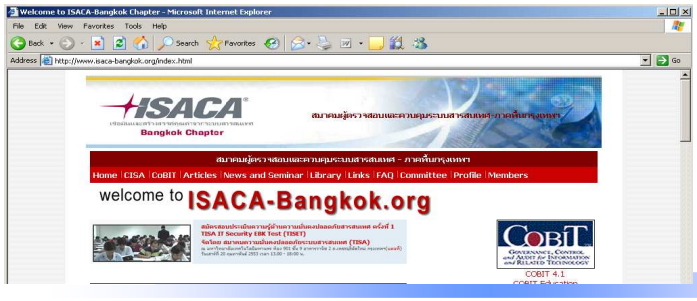
ตลาดหลักทรัพย์แห่งประเทศไทย
The Stock Exchange of Thailand

- Start 1969
- Global organization for information governance, control, security and audit professionals
- Over 65,000 members
- 175 Chapters in 70 countries worldwide
- Administrate CISA CISM and CGEIT certifications
- Established IT Governance Institute (ITGI) in 1998
- More information about ISACA and ITGI
  http://www.isaca.org
  http://www.itgi.org/

About ISACA Bangkok Chapter

ตลาดหลักทรัพย์แห่งประเทศไทย
The Stock Exchange of Thailand

- สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ - ภาคพื้นกรุงเทพฯ
- มีสมาชิก 333 ท่าน (Jan 2010)
- http://www.isaca-bangkok.org
- คุณวรางคณา มุสิกะสังข์ -**Chapter President**



สมาชิกของสมาคม ISACA:

ตลาดหลักทรัพย์แห่งประเทศไทย
The Stock Exchange of Thailand

- ได้รับทราบและแลกเปลี่ยนข่าวสารเกี่ยวกับการควบคุมและตรวจสอบระบบสารสนเทศ เช่น @ISACA
- ได้รับหนังสือวารสาร Journal โดยตรงจากประเทศสหรัฐฯ 6 ฉบับต่อปี(ออกทุก 2 เดือน)
- ได้รับส่วนลดในการเข้าฟังสัมนาที่จัดโดยสมาคมฯ ทั้งในประเทศและต่างประเทศ
- ได้รับส่วนลดในการซื้อจาก ISACA Bookstore
- ได้รับส่วนลดในการสมัครสอบ CISA/CISM/CGEIT
- สามารถดาวโหลดข้อมูล Standard ,Framework, Audit program , ICQ ฯลฯ
- สามารถยืมหนังสือที่มีอยู่ในห้องสมุดของสมาคมฯได้

ที่มาโครงการ

ตลาดหลักทรัพย์แห่งประเทศไทย The Stock Exchange of Thailand

- สืบเนื่องจากกิจกรรมบริการวิชาชีพ คลินิกไอเอ ของ สตท. และ Quarterly Seminar ของ ISACA
- โดยความร่วมมือระหว่าง
  - ตลาดหลักทรัพย์แห่งประเทศไทย
  - สมาคมผู้ตรวจสอบภายในแห่งประเทศไทย
  - สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ – ภาคพื้นกรุงเทพฯ
- จัดประจำต่อเนื่องตั้งแต่ พ.ย. 48
- ให้ความรู้เกี่ยวกับการตรวจสอบ และการควบคุมภายใน

กำหนดการ

ตลาดหลักทรัพย์แห่งประเทศไทย The Stock Exchange of Thailand

9:00	– 9:30	ลงทะเบียน
9:30	– 10:30	เสวนา Internal Fraud
10:30	– 10:45	พักทานกาแฟ อาหารว่าง
10:45	– 12:00	ผู้เข้าร่วมเสวนาซักถาม แลกเปลี่ยนประสบการณ์
12.00		จบการเสวนา

ผู้นำการเสวนา

ตลาดหลักทรัพย์แห่งประเทศไทย The Stock Exchange of Thailand

- คุณศิวะรักษ์ พินิจารมณ์ CPA CIA CFE
  ผู้ช่วยกรรมการผู้อำนวยการสำนักตรวจสอบภายใน บริษัทไทย คม จำกัด(มหาชน)
- คุณไพรัช ศรีวิไลฤทธิ์ CIA CISA CISSP CCSA CFSA CBA CFE
  หัวหน้าตรวจสอบภายใน
  ธนาคารทิสโก้ จำกัด (มหาชน)
- คุณสมชัย แพทย์วิบูลย์
  CIA CISA CISSP PMP Security+ Network+ CEH CFE
  ผู้ตรวจสอบเทคโนโลยีสารสนเทศ
  ธนาคารทิสโก้ จำกัด (มหาชน)

ทุจริตจากภายใน

ผีพนันสิงหนุ่มแบงก์แสบโกง 400 ล้าน

- เดือนพฤษภาคม 2552 ธนาคารตรวจพบสมุห์บัญชีสาขาหนึ่งโอนเงินจากบัญชีดอกเบี้ยที่ธนาคารเตรียมไว้จ่ายลูกค้าเข้าบัญชีตัวเองตามธนาคารต่าง ๆ
- ผู้ต้องหาจนมุมคารถขณะกำลังหนีไปเขมร สารภาพทำมาต่อเนื่องนานกว่า 1 ปี เพราะทำง่ายและไม่เคยถูกตรวจสอบ เงินที่ยักยอกนำไปซื้อบ้าน รถยนต์ เครื่องประดับ ซื้อกองทุน เล่นพนันฟุตบอล ซื้อสลากกินแบ่ง รวมกว่า 499 ล้านบาท
- เริ่มทำงานในธนาคารเมื่อปี 2542 ได้รับรางวัลเป็นพนักงานดีเด่น และไม่เคยมีประวัติการทุจริต
- พบสาเหตุระบบ Core Banking System มีข้อบกพร่อง.

(รูนเศรษฐกิจ 6 พ.ค.52)

อะไรเอ่ยสำคัญเท่าเงินสด

ทายาทเศรษฐีนอนกอดใบหุ้นปลอม 5 ปี

- เดือนธันวาคม 2551 ผู้จัดการมรดกนำใบหุ้นบริษัทจดทะเบียน 672000 หุ้น มาขึ้นทะเบียนกับศูนย์รับฝากหลักทรัพย์เพื่อจัดสรรแก่ทายาท แต่พบว่าเป็นใบหุ้นปลอม
- บริษัทตรวจสอบพบว่าแบบฟอร์มใบหุ้นสามัญหายไป 34 ใบ พนักงานผู้ต้องสงสัยรู้ตัวหลบหนี ใบหุ้นจริงถูกขายไปตั้งแต่ 2547-2548 แต่ผู้ทุจริตปกปิดโดยจ่ายเงินปันผลให้กับผู้ถือใบหุ้นปลอมอย่างต่อเนื่องทุกปี
- บริษัทแจ้งความยกเลิกใบหุ้นที่หาย และแจ้งความดำเนินคดีกับผู้ต้องสงสัย
- บริษัทและผู้บริหารถูกฟ้องเรียกค่าเสียหาย 222 ล้านบาท.

(ไทยรัฐ 21 ก.พ.52)

ไม่แบ่งแยกหน้าที่ต้องเจอดี

อาจารย์หน้ามืด เงินเกษียณหาย 100 ล้าน

- เดือนสิงหาคม 2552 บุคลากรสถาบันศึกษาย่านรังสิตช็อคธนาคารปฏิเสธขึ้นเงินเช็ค 70 ใบที่ออกโดยกองทุนบำเหน็จที่บริหารเอง ทั้งที่ตามรายงานต้องมีเงินในบัญชี 40 ล้าน
- พอถามเจ้าหน้าที่ที่ดูแลกองทุนมาตลอดสิบปี ปัดบอกจะเอาเงินไปเข้าบัญชีให้ แต่กลับหลบหนี จึงรู้ตัวรีบเข้าแจ้งความ
- ผู้ต้องสงสัยสามารถทำรับ-จ่ายเงิน ลงทุน ออกรายงานเองได้ด้วยตัวคนเดียว คาดยักยอกมาหลายปีโดยไม่มีใครรู้ เพราะจ่ายผลประโยชน์ให้ผู้เกษียณหรือลาออกได้ตามปกติ
- บัญชีกองทุนไม่เคยถูกตรวจสอบ สามปีก่อนเคยมีตรวจสอบภายใน แต่รายงานได้สูญหายไป และผู้ตรวจสอบลาออก.

(Network 26 ส.ค.52)

เอาเอกสารมาจากไหน

ต้มแบงก์ 40 ล้าน ปลอมเอกสารมโหฬาร

- วันที่ 11 ธ.ค. 2551 ตำรวจกองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี จับกุมผู้ต้องหาสองคน ขณะติดต่อธนาคารแห่งหนึ่ง สำนักพหลโยธิน
- พบปลอมเอกสารหลักฐาน อำพรางชื่อบุคคลอื่นเพื่อขอสินเชื่อซื้อบ้าน ซื้อรถยนต์ ทำบัตรเครดิต สร้างความเสียหายแก่ธนาคารและสถาบันทางการเงินต่าง ๆ รวมกว่า 40 ล้านบาท รวมทั้งเจ้าของเอกสารที่เดือดร้อนจากการถูกแอบอ้างทั้งที่ตัวเองไม่ได้ก่อหนี้
- ผู้ต้องหาให้การรับสารภาพ และอยู่ระหว่างขยายผลว่ามีพนักงานธนาคารเกี่ยวข้องรู้เห็นด้วยหรือไม่.

(ไทยรัฐ 13 ธ.ค.51)

ตัวอย่างกรณีทุจริต

โจรไฮเทคแฮ็กข้อมูลเชิด 200 ล้าน

- เดือนสิงหาคม 2548 ตัวแทนผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ สังเกตเห็นความผิดปกติใน traffic ของลูกค้าประเภทบัตรเติมเงิน
- สืบพบรหัสข้อมูลของบริษัทถูก hack แล้วนำไป load เงินจำนวนเกินจริงใส่บัตรเติมเงิน เอาไปขายผ่าน Internet ในราคาพิเศษ หรือตั้งโต๊ะให้บริการตามชุมชน
- บริษัทพยายามบล็อกรหัสของบัตรที่ผิดปกติ แต่ก็ยังเสียหายเป็นค่าเสียโอกาสรายได้ สูงถึง 200 ล้านบาท
- จับกุมผู้ต้องหาได้ 4 คน เป็นพนักงานของบริษัทเอง คดียังอยู่ในระหว่างอุทธรณ์.

(ผู้จัดการ 27 ส.ค.48)

จ้างโจรดูแลเงิน

ลากคอยกแก๊ง ฉกเอทีเอ็ม 3 ปี

- วันที่ 15 สิงหาคม 2552 แบงก์ผิดสังเกตสัญญาณเตือนเงินหมดตู้เอทีเอ็มทั้งที่เพิ่งเติมตอนเย็น แจ้งบริษัทขนเงินเข้าตรวจ พบเงินหายจากตู้โดยไม่มีร่องรอยงัดแงะ ส่วนกล้องวงจรปิดถูกคนร้ายใช้ร่มบังจนมองไม่เห็น
- ตำรวจรวบพนักงานบริษัทขนเงินสาขาระยองได้ยกแก๊งรวม 11 คน สารภาพทำมา 3 ปี โดยเติมเข้าตู้เอทีเอ็มไม่ครบและแอบนำไปใช้ส่วนตัว พนันบอล เข้าบ่อนเขมร พอเงินในตู้ใกล้หมด ก็เอาจากตู้อื่นที่รับผิดชอบมาใส่คืนวนไปเรื่อย ๆ
- ตำรวจแจ้งข้อหาร่วมกันลักทรัพย์นายจ้าง คาดความเสียหายเบื้องต้นประมาณ 23 ล้านบาท.

(ไทยรัฐ 18 ส.ค. 52)

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, contactors, 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.

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

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

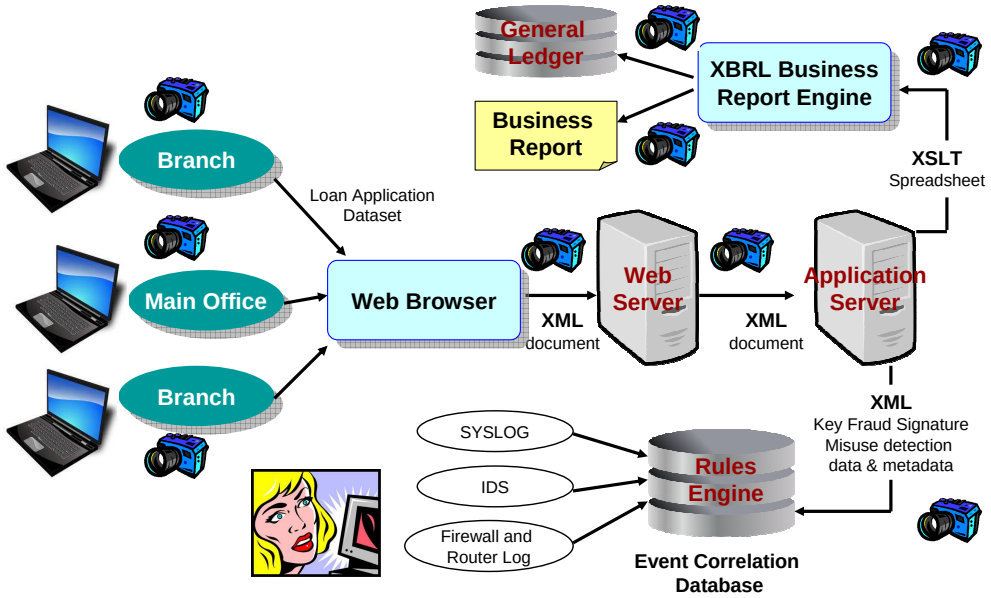
Access Controls
- Identification & Authentication
- Authorization
- Accountability
- Audit
- Physical Devices (i.e. biometric scan, metal locks, hidden path, digital signatures, encryption, social barriers, human and automated monitoring systems etc.),
- Permit or deny use of an object

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

Auditor's 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

About the ACFE

ACFE Association of Certified Fraud Examiners

- The Association of Certified Fraud Examiners
- Start 1988
- Provide anti-fraud training and education
- Over 50,000 members in 125 countries
- Administrate the Certified Fraud Examiner (CFE) designation- a certification program for fraud practitioners recognized by U.S. Department of Defense and FBI
- More than 20,000 CFE's worldwide (5 Thais)
- $55 Membership Fee
- More information about ACFE http://www.acfe.com

About CFE Exam

ACFE Association of Certified Fraud Examiners

- Covers 4 areas
  - Criminology & Ethics
  - Financial Transactions
  - Fraud Investigation
  - Legal Elements of Fraud
- 4 Exam sections of 125 questions each (75%)
- Administered via computer / must complete each section in one sitting (2.6 hr)
- Complete all and return to ACFE in 30 days
- Must pass Qualifying Points System (40/50)
- $250 Application Fee