Unit 7 of Part II

Specific IT Engagements

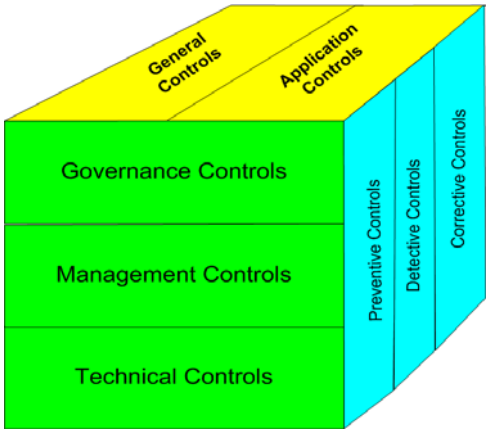
Manit Panichakul CIA, CISA, CISM
June 19, 2011

Agenda

1. Electronic Funds Transfer (EFT)
2. Electronic Data Interchange (EDI)
3. E-Commerce
4. Information Protection
5. Encryption
6. Enterprise-Wide Resource Planning (ERP)
7. Computer-Assisted Audit Techniques (CAAT)
8. Questions

Understanding Controls

- **Classification**
  - General Controls
  - Application Controls
- **Classification**
  - Preventative
  - Detective
  - Corrective
- **Classification**
  - Governance controls
  - Management controls
  - Technical controls



Automated vs Manual

Automated controls, generally operate consistently. Therefore, a periodic reconfirmation through evaluation of a single instance of automated controls is often an acceptable monitoring threshold. In such situations, management includes in its monitoring procedures the effectiveness of its program testing, program security, and change-control processes.

Manual controls, the quantity of information necessary will vary depending on the frequency of a control's operation.>>Prone to error/human error

1. EFT

- **Electronic funds transfer (EFT)**
  - Provide by financial institution based on EDI technology
  - Costs are lower than manual transactions
  - Typical app is the direct deposit of payroll checks
  - Dirct Credit/Direct Debit services
  - The most important app is check collection (can reduce enormous volume of paper
  - Eg., Federal Reserve wire transfer network (Fedwire) and New York Clearing House Interbank Payment System (CHIPS)
- **Implications for IA**
  - Elimination of paper documents
  - Existence of evidence
  - Evaluation of digital signatures
  - Consideration of other subsystems/interfaces

2. EDI

- **Electronic Data Interchange (EDI):** communication of electronic documents directly among entities. The first step of e-business evolution that was developed to enhance JIT.
- **Risk**
  - Security of info: End-to-End encryption
  - Loss of data
- **EDI terms and components**
  - Standards – procedure to convert written doc to a standard electronic document-messaging format
  - Conventions: procedure for arranging data elements in specified formats e.g., invoices, shipment notices

2. EDI

- **EDI terms and components (cont)**
  - Data dictionary: meaning of data elements
  - Transmission protocols: rule how electronic envelope is structured and processed
  - Large company may force trading partners to adopt its standards
- **Methods of communication**
  - Point-to-Point
  - Value-added networks (VAN): private mail box services with hardware encryption e.g. Host Security Module (HSM)
  - Internet (cost advantage): less formal agreement/sending doc in format of receiving firm
- **Implication to IA**
  - Also eliminate even the electronic equivalents of paper docs (full advantage of EDI)
  - Point-of-Sale (POS) provide direct transmission (buyer/seller):

2. EDI

- **Implication to IA (cont)**
  - New form of Evidence: authorized paper purchase contract and receipts settlement
  - To evaluate digital signatures and test of controls and interfaces
- **EDI controls**
  - Authorized users with independence access (initiate, authorize, parties, and senders for exceptional transactions)
  - Message authentication: smart card and other hardware software techniques
  - Message protection from interception or tampering: controls:-
    - Encryption,
    - Numerical Sequencing,
    - Non-repudiation (digital certificates to prove origination&delivery, acknowledgement and confirmation in web site dialogue to avoid later disputes)
- **Secure Electronic Transaction (SET): control over non-repudiation is achieved by sequencing, encryption and authentication.**

3. E-Commerce

Electronic Commerce (E-Commerce)

- The purchase and sale of goods and services by electronic means
- E-business: a more comprehensive term with all methods of conducting business electronically
- E-commerce: online transactions on public networks, electronic data interchange (EDI), and email
- Security issues
  - Authentication: the correct identification of the transaction parties
  - Authorization: who may rightfully make decision (entering into contract, setting prices

3. E-Commerce

- Security issues
  - Protecting methods for confidentiality&integrity of info
    - Evidence of transmission and receipt of document
    - Guarding against repudiation by sender or recipient
  - Trustworthiness of listed prices and confidentiality of discounts
  - Confidentiality and integrity of orders, payments, delivery addresses and confirmation
  - Proper extent of verification of payment data
  - The best method of payment to avoid wrongdoing and disagreements
  - Lost or duplicated transactions
  - Who bears the risk of fraud

3. E-Commerce

- Control for response to the Security issues
  - Encryption/Authentication
  - Adherence to legal requirement
  - Documenting trading agreements e.g., term of trade, methods of authorization and authentication
  - Agreements for end-to-end security and availability
  - Disclose by public trading systems of their terms of business
  - Capacity of host to avoid downtime and attacks

3. E-Commerce

Electronic Commerce (E-Commerce)

- Conducting commercial activities over the Internet: B2B business-to-business, B2C business-to-consumer, B2E business-to-employee
- Impacted by new threats: web-based and other technology changes>fraud, authentication, data corruption, business interruption/BCP
- Internal and External Assurance

3. E-Commerce

Competency and capacity of IAA: limiting factors

- Sufficiency of skills
- The need for training and other resources
- Long term/short term staffing levels
- Deliverability of the expected audit plan
- Regulatory issues

3. E-Commerce

- **Risk&control issues:**
  - Threat event that could adversely affect the achievement of objectives and execute strategies – review the existence of a business plan
  - New threats and changes in technology
  - Single loss exposure values (make financial impacts)
  - Frequency/probability
  - Uncertainty
  - Safeguards and controls (including cost)
  - Cost/benefit or ROI analysis
  - Critical risk and control,

3. E-Commerce

- **Critical risk and control,**
  - Security threat and technology changes
  - Fraud
  - Authentication: 2 factors or multi-factors authentication (knowledge&possession)

  >>>OTP-One Time Password
  - Corruption of data/business interruptions
  - Management issues, business model, economical review

4. Information Protection

- **Critical risk,**
  - Security awareness
  - Operational control over access, change management, should be inplace to achieve the objective of Protectability
  - Malware or malicious software
    - Trojan horse – hidden function that may do damage when activated >>virus (from file to file), worm (from PC to PC)
  - Logic Bomb: like trojan horse but activated only upon some occurrence e.g., Friday 13
  - DoS – Denial of Service: too much traffic to handle

4. Information Protection

- **Overall Audit Objective:**
  - **Enterprise must put in place - IT Security Policy, Antivirus software, email attachment should be scanned and documentation of effective control:-**
    - **Evidence of transaction/timeliness of info**
    - **Availability/reliability of security**
    - **Effective interface with financial systems**
    - **Security of monetary transactions**
    - **Effectiveness of customer authentication**
    - **BCM/Public-key certificates/digital signatures**

5. Encryption

- **Plaintext VS Cyphertext**
  - **Encryption technology converts data into a code.**
  - **Encryption software uses a fixed algorithm to manipulate Plaintext and an encryption key to introduce variation. The encryption key is necessary to understand /decrypt the data**
  - **Hardware or software-based encryption**

5. Encryption

- **Public Key**
  - Or Asymmetric ,encryption requires two keys.
  - For coding messages (Public Key)
  - For decoding messages (Private Key)
  - One advantage of Public Key encryption is that the messages in encoded using one key and decoded using another
  - The second advantage is that neither party knows the other's Private key
  - The related Public Key/Private Key are issued by a Certificate Authority (CA-3rd Party) fiduciary e.g., VeriSign or Thawte
  - Key management a Public Key system is more secure than in a secret key system

5. Encryption

- **Public Key**
  - RSA (Rivest, Shamir, Adelman), is the most commonly used public key method
  - Digital Signatures (fingerprints)
    - Is a mean of authentication of an electronic document, e.g., validity of PO, acceptance of a contract or financial info
    - Digital Certificate is another means of authentication used in e-business
    - Public Key infrastructure permits secure monetary and info exchange over Internet
    - SSL (Secure Sockets Layer) and S-HTTP (Secure Hypertext Transport Protocol)
    - Digital time stamping service verify the time (Place) of a transaction

5. Encryption

- **Private Key**
  - **or symmetric, encryption requires only a single (secret) key for each pair of parties**
    - **Data Encryption Standard (DES) , a shared private key method developed by the US GOV**
    - **Advanced Encryption Standard (AES) is a recently adopted cryptographic algorithm for use by US GOV to protect sensitive info (voluntary basis)**
    - **TDES-Triple DES is stronger than Single DES**

6. Enterprise-wide Resource Planning

- **What is ERP:** the latest phase in the development of computerized systems for managing the org resources by integrate info in one data base link to applications
- **Traditional ERP system:** with back-office functions can produce info principally for internal use
- **Enterprise Resource Planning (ERP II):** the current version of ERP software (front office function was added)
  - Supply-chain management
  - Customer relationship management (CRM) with busuness intelligence software
  - Partner relationship management
- **Current ERP software (ERP):** SAP R/3, Oracle, PeopleSoft and J.D.Edwards
- Effective change management is required for success

6. Enterprise-wide Resource Planning

- ERP architecture
  - Client-server configuration
  - Central database
  - Implementation of ERP
    - Project team
    - Strategic planning
    - ERP software choosing and consulting firm selection
    - Preimplementation
    - Go-live
    - Training
  - Costs & Benefit of an ERP

6. Enterprise-wide Resource Planning

- ERP architecture
  - Client-server configuration
  - Central database
  - Implementation of ERP
    - Project team
    - Strategic planning
    - ERP software choosing and consulting firm selection
    - Preimplementation
    - Go-live
    - Training
  - Costs & Benefit of an ERP

7. การประยุกต์ใช้คอมพิวเตอร์เพื่อช่วยในการตรวจสอบ

ประโยชน์ของการใช้ CAATs

- ทำให้เห็นภาพรวมของระบบและการเคลื่อนไหวของรายการ
- ช่วยในการจัดการกับข้อมูลเหล่านั้น ได้แก่
  - การจัดประเภท (classify)
  - การแยกประเภท (stratify)
  - การวิเคราะห์ทางสถิติ และคณิตศาสตร์ (statistic &mathematic analysis)
- ช่วยให้การวิเคราะห์รายการที่ผิดปกติง่ายยิ่งขึ้น
- ผู้ตรวจสอบจำเป็นต้องใช้ CAATs ในการตรวจสอบระบบที่ใช้เทคโนโลยีสารสนเทศเพื่อการประมวลผล (General Controls & Application Controls Review)

7. การประยุกต์ใช้คอมพิวเตอร์เพื่อช่วยในการตรวจสอบ

ประโยชน์ของการใช้ CAATs

- ช่วยลดระดับความเสี่ยงซึ่งเกิดจากการตรวจสอบ
- ช่วยเพิ่มความเป็นอิสระจากผู้รับการตรวจสอบ >>to obtain audit evidence
- สามารถเพิ่มขอบเขตการตรวจสอบให้ครอบคลุมมากยิ่งขึ้น
- ช่วยเพิ่มโอกาสในการประเมินและวิเคราะห์เชิงปริมาณเพื่อค้นหาจุดอ่อนของการควบคุม
- ช่วยเพิ่มประสิทธิภาพในการสุ่มตัวอย่าง
- เพิ่มประสิทธิผลในการตรวจสอบในกรณีการตรวจสอบสิ่งผิดปกติ/รายการทุจริต
- ลดค่าใช้จ่ายและระยะเวลาในการตรวจสอบ

1). Historical Data Techniques

วิธีการตรวจสอบ โดยนำข้อมูลชุดที่ผ่านการปฏิบัติจริงมาทำงานด้วยชุดโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นเพื่อการทดสอบ ได้แก่ เทคนิค ดังต่อไปนี้

1.1 Parallel Simulation
1.2 Extended Record
1.3 Transaction Selection
1.4 Generalized Audit Software

2). Concurrent Data Techniques

วิธีการตรวจสอบการทำงานของชุดโปรแกรมคอมพิวเตอร์ พร้อมๆกับการทำงานของระบบงานที่เป็น Production Run สามารถตรวจสอบได้ทันทีที่เกิดรายการ ได้แก่ เทคนิค ดังต่อไปนี้

2.1 Integrated Test Facilities
2.2 Embedded Module (SCARF)
2.3 Logging
2.4 Tagging
2.5 Monitoring

3). Programmed Analysis Techniques

วิธีการตรวจสอบการทำงานของโปรแกรมบางส่วนหรือ ทั้งหมดว่า Function เหล่านั้นเป็นไปตามที่กำหนดหรือไม่

3.1 Test Data Method

3.2 Base Case System Evaluation

3.3 Snap Shot

3.4 Mapping

3.5 Tracing

การใช้โปรแกรมสำเร็จรูปสำหรับการตรวจสอบทั่วไป

- **GAS เป็นโปรแกรมสำเร็จรูปที่พัฒนาขึ้นเพื่อใช้ในการตรวจสอบทั่วไป**
- **GAS ที่นิยมใช้กันทั่วไปได้แก่**
  - **IDEA (Interactive Data Extraction and Analysis)** และ
  - **ACL (Audit Command Language)**
- **GAS ช่วยให้ผู้ตรวจสอบสามารถหาหลักฐานเกี่ยวกับคุณภาพของเรคคอร์ด (record) ข้อมูลต่างๆ ได้โดยตรง ซึ่งมีส่วนในการตัดสินใจเกี่ยวกับคุณภาพและการควบคุมภายในของโปรแกรมประยุกต์ว่ามีความน่าเชื่อถือเพียงใด**

สาเหตุที่ทำให้เกิดมีการพัฒนา GAS

- เกิดจากการนำระบบคอมพิวเตอร์มาใช้มากขึ้น ผู้ตรวจสอบประสบกับปัญหาความหลากหลายของซนิดซอฟต์แวร์ และ ฮาร์ดแวร์ที่ผู้รับการตรวจใช้ซึ่งผู้ตรวจสอบจำเป็นต้องดึงข้อมูลที่จัดเก็บมาตรวจสอบ
- ประโยชน์ที่จะได้รับจากการใช้ **GAS** คือ
  - ช่วยประหยัดเวลาที่ใช้ในการเขียนโปรแกรมเพื่อการตรวจสอบระบบได้
  - สามารถทำได้อย่างรวดเร็ว ในกรณีที่มีการเปลี่ยนวัตถุประสงค์ในการตรวจสอบ **(audit objectives)**
  - ผู้ตรวจสอบที่ไม่มีความชำนาญในเรื่องการเขียนโปรแกรมก็สามารถใช้ **GAS** ได้

ความสามารถในการทำงานของ GAS

- การเข้าถึงแฟ้มข้อมูล **(File Access)**
- การจัดเรียงข้อมูลใหม่ **(File Reorganization)**
- การเลือกรายการ **(Selection)**
- การคำนวณทางสถิติ **(Statistical)**
- การคำนวณทางคณิตศาสตร์ **(Arithmetic)**
- การแบ่งข้อมูลเป็นลำดับชั้นและวิเคราะห์ความถี่ **(Stratification and Frequency Analysis)**
- การสร้างแฟ้มข้อมูลใหม่ และ การปรับให้เป็นปัจจุบัน **(File Creation and Updating)**
- การจัดทำรายงาน **(Reporting)**

ข้อจำกัดของ GAS

- ข้อจำกัดในการช่วยงานตรวจสอบอยู่ 4 ประการที่สำคัญ คือ
  - **GAS** สามารถตรวจสอบได้เฉพาะหลังจากเกิดรายการแล้ว **(ex post auditing)** เท่านั้น
  - **GAS** สามารถตรวจสอบ **processing logic** ได้ในกรณีที่ **logic** ไม่สลับซับซ้อนมากนัก แต่ในกรณีที่ **logic** มีความสลับซับซ้อนอาจจะไม่คุ้ม
  - **GAS** ไม่สามารถบอกถึงแนวโน้มที่ระบบอาจมีข้อผิดพลาด
  - **GAS** จำเป็นต้องใช้ข้อมูลจากระบบโดยให้ความเชื่อถือว่าข้อมูลที่ได้มามีความครบถ้วนและสมบูรณ์

การใช้ข้อมูลทดสอบ

- *การใช้ข้อมูลทดสอบ มี 2 ประเภทที่สำคัญคือ*
- การใช้ข้อมูลทดสอบ แบบเทสท์ดาต้า **(Test Data)** ซึ่งเป็นวิธีที่ออกแบบขึ้นมาเพื่อใช้กับการประมวลผลแบบกลุ่ม (การประมวลผลแบบกลุ่ม **(Batch processing)**)
- การใช้ข้อมูลทดสอบแบบอินทีเกรเต็ดเทสท์ฟาซิลิตี้ **(Integrated Test Facility)**

ขั้นตอนในการทำเทสท์ดาต้า

- สอบทานเอกสารประกอบระบบของลูกค้า เพื่อดูว่าจุดควบคุมมีอะไรบ้าง
- สร้างข้อมูลทดสอบหรือรายการจำลอง **(Simulated transactions)**
- บันทึกรายการลงในกระดาษทำการของผู้ตรวจสอบ พร้อมที่คำนวณผลการประมวลผลที่คาดว่าจะได้รับ **(Predetermined computer results)** ด้วยมือ แล้วบันทึกลงในกระดาษทำการ
- ทำการประมวลผลโดยใช้โปรแกรมคอมพิวเตอร์ของลูกค้าโดยทำบนเครื่องคอมพิวเตอร์ของผู้ตรวจสอบ แล้วนำผลการประมวลที่ได้ไปเทียบกับที่คำนวณไว้ล่วงหน้า

ข้อดีและข้อเสียของการใช้เทสท์ดาต้า

- **ข้อดี**
  - ผู้ตรวจสอบมีความมั่นใจมากขึ้นในความเชื่อถือได้ของโปรแกรมที่ผู้รับการตรวจใช้ปฏิบัติงาน
- **ข้อเสีย**
  - ไม่สามารถทำให้แน่ใจว่าการควบคุมภายในมีประสิทธิผล
  - โปรแกรมที่ผู้ตรวจสอบตรวจสามารถทำงานตามที่ควรเฉพาะที่อยู่ในขอบเขตของ **Test data** เท่านั้น
  - สามารถทดสอบจำกัดเพียงฟังก์ชันที่มีอยู่ในโปรแกรมของลูกค้า
  - เหมาะสำหรับการประมวลผลแบบกลุ่ม **(Batch processing)** เท่านั้น
  - การพัฒนา **Test Data** ต้องใช้เวลามากและต้องปรับให้เข้ากับแอปพลิเคชั่น **(Application)** แต่ละอัน

การใช้ข้อมูลทดสอบแบบอินทีเกรเต็ดเทสท์ฟาซิลิตี้

- เป็นเทคนิคซึ่งผู้ตรวจสอบ สร้างข้อมูลจำลองขึ้น **(Simulated transaction)** แล้วนำไปประมวลผลร่วมกับข้อมูลจริงของลูกค้าโดยใช้ โปรแกรมประยุกต์ **(Application program)** ซึ่งลูกค้าใช้ในการประมวลผลข้อมูลตามปกติบนเครื่องคอมพิวเตอร์ที่ลูกค้าใช้งานอยู่จริง หลังจากการประมวลผลจะนำผลที่ได้มาวิเคราะห์
- ข้อเสีย
  - โปรแกรมประยุกต์ **(Application program)** ของลูกค้าอาจถูกแก้ไขให้ทำการประมวลผลข้อมูลที่เป็นข้อมูลจำลอง **Dummy** (ซึ่งมีรหัสพิเศษ) ต่างจากการประมวลผลข้อมูลจริง
  - การใส่ และลบข้อมูลจำลองอาจทำให้เกิดข้อผิดพลาดขึ้นในข้อมูลจริงได้โดยไม่ได้ตั้งใจ

>>**dummy transaction must be purged prior to internal and external reporting. Not used extensively by external auditors.**

แมปปิ้ง (Mapping)

- เป็นเทคนิคในการติดตามคำสั่งในการทำงานและชี้ถึงการให้คำสั่งที่ไม่ถูกใช้ โดยจะมีการแสดงรายละเอียดถึงจำนวนครั้งและระยะเวลาในการทำงาน
- ใช้เป็นเครื่องมือในการปรับปรุงการเขียนโปรแกรมอย่างมีประสิทธิภาพ
- ช่วยให้ตรวจพบ ส่วนของคำสั่งที่เป็นไทม์บอมบ์ **(time bomb)** หรือม้าโทรจัน **(trojan horse)** โดยดูจากคำสั่งที่ไม่เคยมีการเรียกใช้

>>tracing and mapping verifies source code (not actual production data)

การใช้ภาษาระดับสูง (High-Level Language)

- ภาษาโปรแกรมยุคที่หนึ่ง 1GL - **First-generation programming language:** ภาษาเครื่อง **(Machine language)**
- ภาษาโปรแกรมยุคที่สอง 2GL - **Second -generation programming language:** ภาษาแอสเซ็มบลี **(Assembly language)**
- ภาษาโปรแกรมยุคที่สาม 3GL - **Third -generation programming language:** ภาษาที่ต้องใช้ทักษะโปรแกรมเมอร์ **(Procedural language)**
- ภาษาโปรแกรมยุคที่สี่ 4GL - **Fourth-generation programming language:** ภาษาที่ไม่ต้องใช้ทักษะโปรแกรมเมอร์ **(Non-procedural language)** เป็นการใช้ภาษาระดับสูง (ใกล้เคียงกับภาษามนุษย์ เช่นภาษาอังกฤษ)
- ภาษาโปรแกรมยุคที่ห้า 5GL - **Fifth-generation programming language:** ภาษาที่มีองค์ประกอบของปัญญาประดิษฐ์ **(Artificial Intelligence)** หรือ เอไอ **(AI) >>expert system**

Questions

1.Which of the following conditions is not a condition that the internal auditor should be alert for when testing for fraud in an e-commerce audit?

a.Denial of service attacks.
b.Duplication of payments.
c.Denial of orders placed or received.
d.Exception reports and procedures.

Questions

2. With respect to business interruptions, what is the most crucial element of business recovery?
   a. Information systems backup.
   b. Alternative communication systems and site facilities.
   c. Business impact assessments and resumption plans.
   d. Disaster recovery plan.

Questions

3. What risk element is management seeking to identify by asking: What could happen that would adversely affect the organization's ability to achieve its objectives and execute its strategies?
   a. Single loss exposure value.
   b. Safeguards and controls.
   c. Threat events.
   d. Frequency.

Questions

4. Electronic commerce (e-commerce) is generally defined as “conducting commercial activities over the Internet.” These commercial activities can be all but which of the following?

   a. Business-to-business.
   b. Business-to-consumer.
   c. Business-to-employee.
   d. Consumer-to-business.

Questions

5. With regard to e-commerce, risk is best defined as

   a. The uncertainty of an event occurring that could have a negative impact on the achievement of objectives.
   b. The uncertainty of an event occurring that could positively impact management’s ability to safeguard organizational assets.
   c. The uncertainty of an event occurring that could have a positive impact on the achievement of objectives.
   d. The uncertainty of an event occurring that could have an impact on the effective and efficient use of an organization’s resources.