Control Audit & Security of IS

LEARNING GOALS

- ƒ Why controls are necessary in Information systems?
- ƒ Methods of controlling Information systems?
- ƒ How controls are introduced in Information systems?
- ƒ Why Information systems need auditing?
- ƒ How are systems audited?
- ƒ How the security of an Information system is ensured?

MOTIVATION FOR CONTROLS

- ƒ It is very important to ensure the reliability of reports produced by an information system
- ƒ If unreliability is seen by users the entire credibility of the system is lost
- ƒ Ensuring reliability is not difficult for small systems but when a system has to handle massive data it is a challenge
- ƒ Systematic controls are thus essential when a system is designed

MOTIVATION FOR AUDITS

- Many organizations are now entirely dependent on computer based information system
- ƒThese information systems contain financial data and other critical procedures
- ƒIt is essential to protect the systems against frauds and ensure that sound accounting practices are followed
- ƒIt is necessary to trace the origin and fix responsibilities when frauds occur
- ƒ Audit methods primary purpose is to ensure this.

MOTIVATION FOR SECURITY

- ƒ Systems contain sensitive data about the organization and also about persons working in the organization
- ƒ Sensitive data should be protected from spies, thieves or disgruntled employees.
- ƒThus access should be carefully controlled and provided only on a need to know basis
- ƒWhen computers are networked corruption/erasure may take place due to viruses Services may be disrupted due to denial of service attacks
- ƒ Thus systems should be designed with appropriate security

CONTROL AUDIT AND SECURITY OF INFORMATION SYSTEM

CONTROL- Method to ensure that a system processes

data as per design and that all data is included and are correct

AUDIT AND TESTING - Ensure that the system is built

as per specifications and that processed results are correct.

- Protect systems from frauds.

SECURITY- Protection of data resources, programs , and

equipment from illegal use , theft , vandalism , accidents,

disasters etc.

NEED OF CONTROLS

- Information systems handle massive amounts of data – accidents such as not including some data can cause serious damage
- Incorrect data entry can lead to high monetary losses
- Credibility in the information system may be lost if errors are found in operational systems

OBJECTIVES OF CONTROLS

- To make sure data entering the computer are correct
- Check clerical handling of data before it is input to a computer
- Provide means of detecting and tracing errors which occur due to bad data or bad program
- Ensure legal requirements are met
- To guard against frauds

Information systems controls

General controls

- Govern design, security, and use of computer programs and data throughout organization’s IT infrastructure
- Combination of hardware, software, and manual procedures to create overall control environment

Types of general controls

- **Software controls**
- **Hardware controls**
- **Computer operations controls**
- **Data security controls**
- **Implementation controls**
- **Administrative controls**

Information systems controls

Application controls

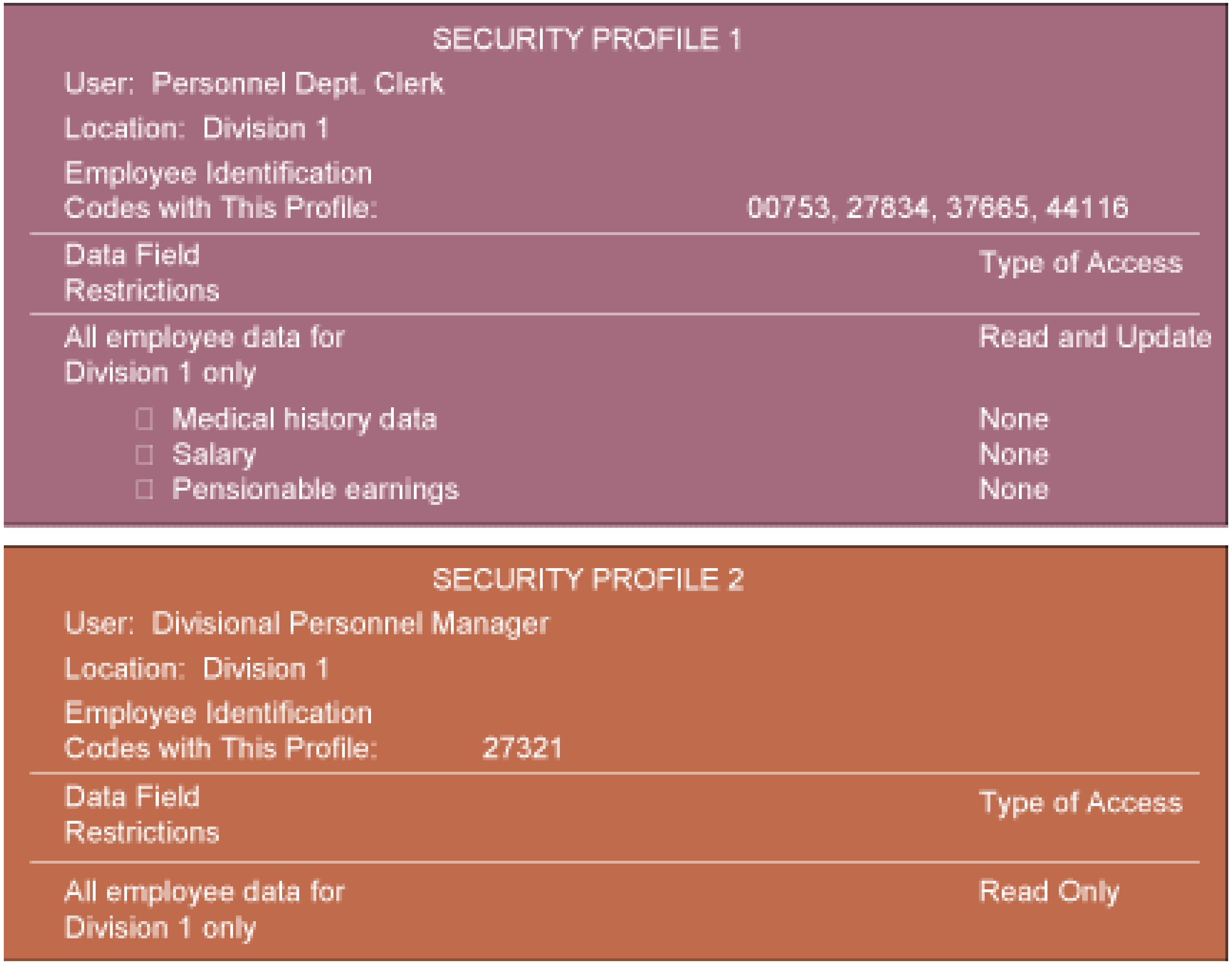
- Specific controls unique to each computerized application, such as payroll or order processing
- Include both automated and manual procedures
- Ensure that only authorized data are completely and accurately processed by that application

Types of application controls:

  - **Input controls**
  - **Processing controls**
  - **Output controls**

Example : General Control

Security Profiles for a Personnel System



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification
Codes with This Profile: 00753, 27834, 37665, 44116

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
□ Medical history data	None
□ Salary	None
□ Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee Identification
Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

Example :Application Control-Protecting the Digital Firm

- On-line transaction processing: Transactions entered online are immediately processed by computer

- Fault-tolerant computer systems: Contain extra hardware, software, and power supply components

Example :Application Control- Protecting the Digital Firm contd…

- High-availability computing: Tools and technologies enabling system to recover from a crash

- Disaster recovery plan: Runs business in event of computer outage

- Load balancing: Distributes large number of requests for access among multiple servers

Example :Application Control- Protecting the Digital Firm contd…

- Mirroring: Duplicating all processes and transactions of server on backup server to prevent any interruption

- Clustering: Linking two computers together so that a second computer can act as a backup to the primary computer or speed up processing

Example :Application Control-Protecting the Digital Firm contd…

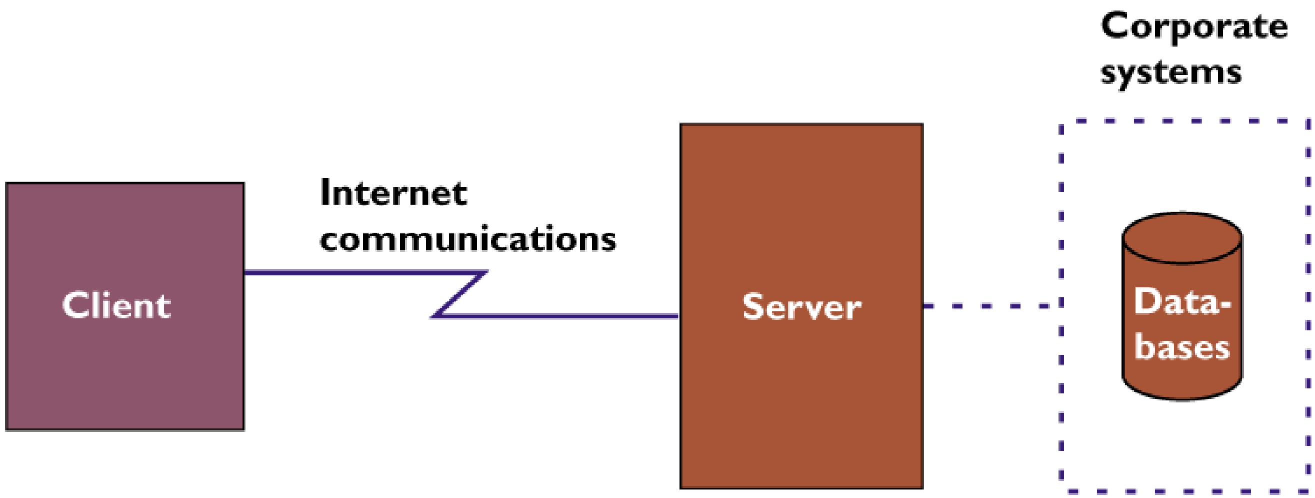
Firewalls

- Prevent unauthorized users from accessing private networks
- Two types: proxies and stateful inspection

Intrusion Detection System

- Monitors vulnerable points in network to detect and deter unauthorized intruders

Internet Security Challenges



- Computer viruses
- Line taps
- Loss of machine

- Tapping
- Sniffing
- Message alteration
- Theft and fraud

- Hacking
- Computer viruses
- Theft and fraud
- Line taps
- Vandalism
- Denial–of–service attacks

- Theft of data
- Copying of data
- Alteration of data

Security and Electronic Commerce

- Encryption: Coding and scrambling of messages to prevent their access without authorization

- Authentication: Ability of each party in a transaction to ascertain identity of other party

- Message integrity: Ability to ascertain that transmitted message has not been copied or altered

Security and Electronic Commerce

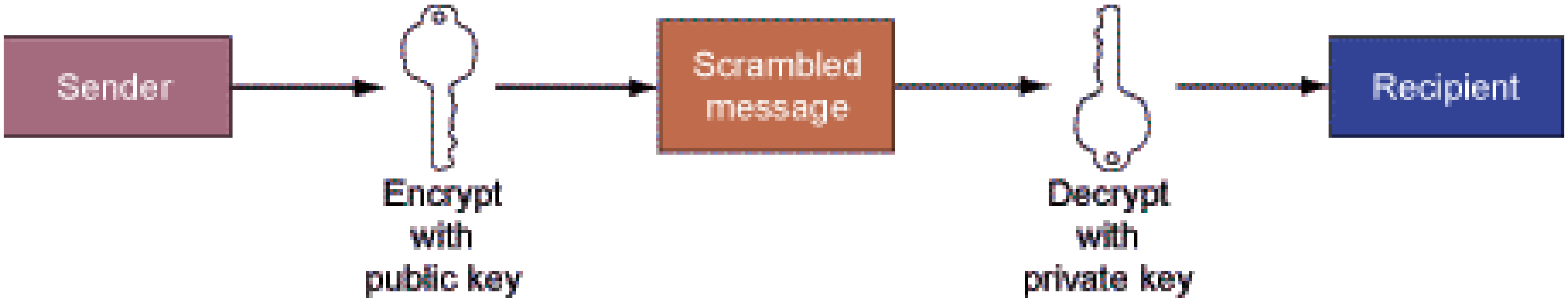
- Digital signature: Digital code attached to electronically transmitted message to uniquely identify contents and sender

- Digital certificate: Attachment to electronic message to verify the sender and to provide receiver with means to encode reply

Security and Electronic Commerce

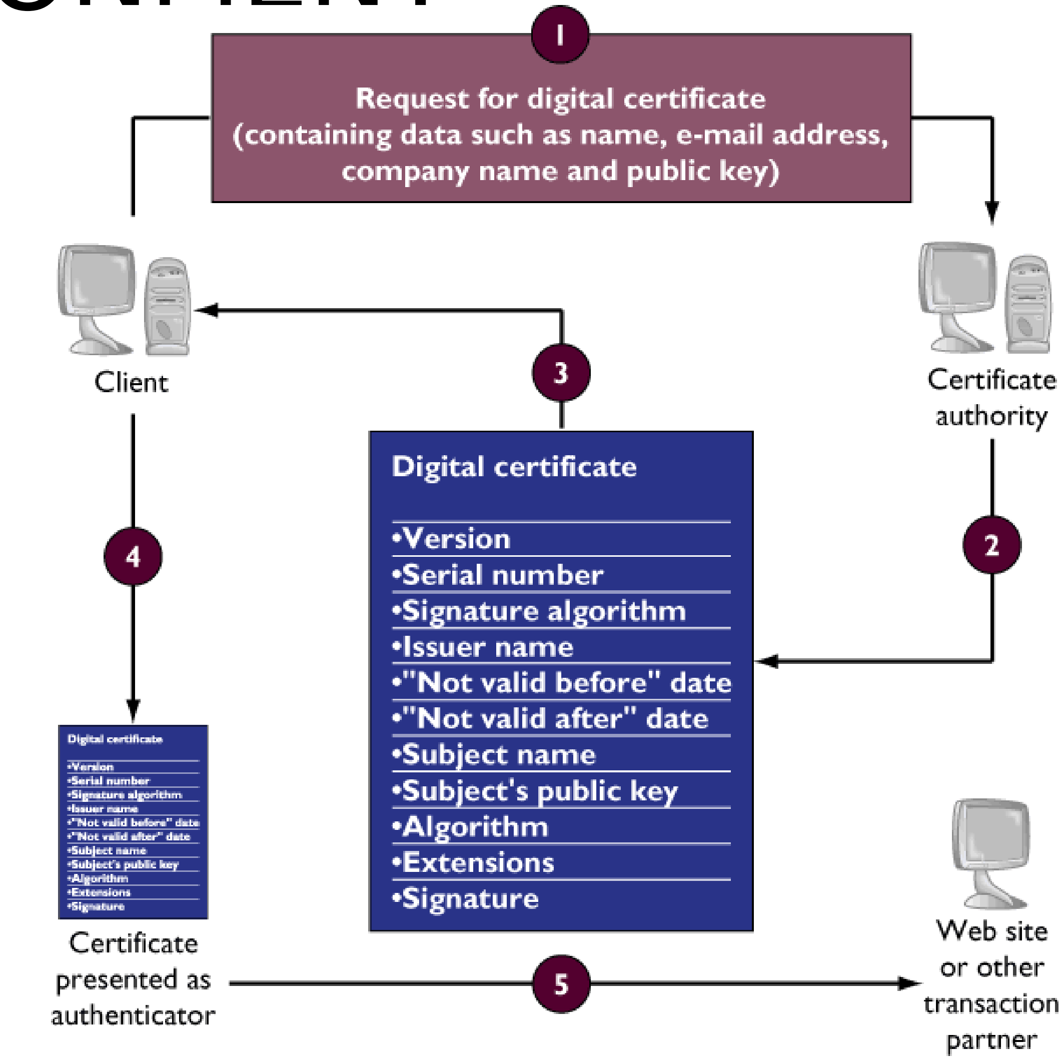
- Secure Electronic Transaction (SET): Standard for securing credit card transactions over Internet and other networks

Public Key Encryption



CREATING A CONTROL ENVIRONMENT

Digital Certificates



1 Request for digital certificate (containing data such as name, e-mail address, company name and public key)

Client

Certificate authority

2

3

Digital certificate

- •Version
- •Serial number
- •Signature algorithm
- •Issuer name
- •"Not valid before" date
- •"Not valid after" date
- •Subject name
- •Subject's public key
- •Algorithm
- •Extensions
- •Signature

4

Certificate presented as authenticator

5

Web site or other transaction partner

Developing a Control Structure: Costs and Benefits

Criteria for determining control structure

- Importance of data
- Efficiency, complexity, and expense of each control technique
- Level of risk if a specific activity or process is not properly controlled

The Role of Auditing in the Control Process

MIS audit

- Identifies all controls that govern individual information systems and assesses their effectiveness

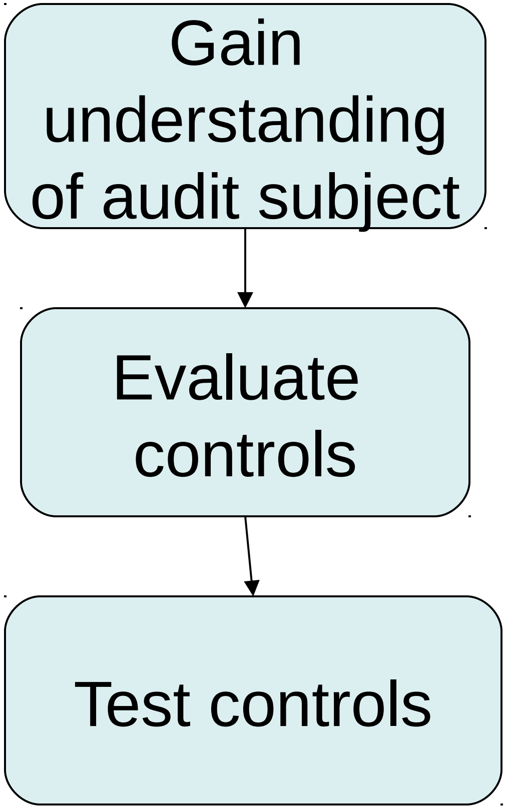
AUDITING OF INFORMATION SYSTEMS

OBJECTIVES

- ƒ Ensure computer based financial and other information reliable
- ƒ Ensure all records included while processing
- ƒ Ensure protection from frauds

IS Audit Definition

IS Audit: Any audit that wholly or partially evaluates automated information processing system, related non-automated processes, & their interfaces



Simplified Audit Process

Audit Planning

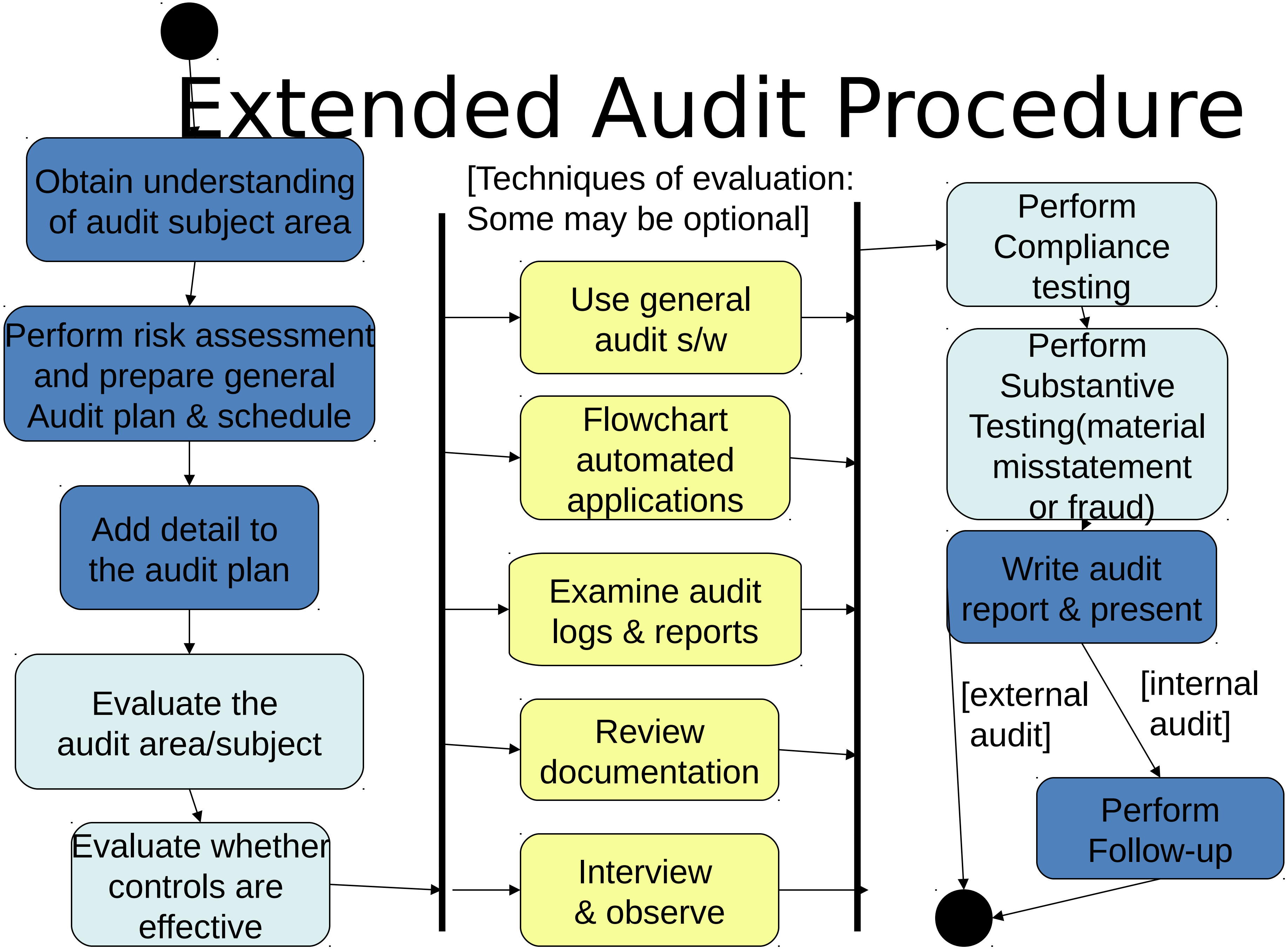
- **Short-Term**: What do we need to audit this year?
- **Long-Term**: What should we plan to audit in the future?
- What should we test first? Consider…
  - What parts of our business are the most susceptible to risk?
  - What business/IS systems are changing?
  - Are new evaluation tools available?
  - What regulations must we test for?
  - Are there new regulations to test for?

Workbook

Audit Planning Table

Audit Area	Time-frame	Date of Last Test	Responsibility
Policies & Procedures for Registration, Advising	1Q	Never	Internal Auditor
Business Continuity	2Q	2005	CIO, Security Consultant
FERPA: Personnel interviews	3Q	Never	Internal Auditor
IT: Penetration Test	4Q	2006	CIO, Security consultant

Extended Audit Procedure



Obtain understanding of audit subject area

Perform risk assessment and prepare general Audit plan & schedule

Add detail to the audit plan

Evaluate the audit area/subject

Evaluate whether controls are effective

[Techniques of evaluation: Some may be optional]

Use general audit s/w

Flowchart automated applications

Examine audit logs & reports

Review documentation

Interview & observe

Perform Compliance testing

Perform Substantive Testing(material misstatement or fraud)

Write audit report & present

[external audit]

[internal audit]

Perform Follow-up

Step 1: Obtain Understanding of Audit Subject Area

May include:

- Tour facilities related to audit
- Read background material
- Review business and IT strategic plans
- Interview key managers to understand business
- Review prior audit reports
- Identify applicable regulations
- Identify areas that have been outsourced

Step 2: Perform Risk Assessment

Risk-Based Auditing

Inherent Risk: Susceptibility to a problem

- E.g., a bank’s inherent risk is a robber

Control Risk: A problem exists that will not be detected by an internal control system

- For bank: A thief accesses another’s account at Money Machine but is not detected

Detection Risk: An auditor does not detect a problem that does exist

- For bank: Fraud occurs but is not detected

Overall Audit Risk: Combination of audit risks

Step 2: Prepare Audit Plan

- Develop risk-based approach
- Include audit objectives, scope, timing, required resources
- Comply with applicable law
- Develop audit program and procedures

Audit Plan Vocabulary

Audit Subject: The area to be audited

- E.g., Information Systems related to Sales

Audit Objective: The purpose of the audit

- E.g., Determine whether Sales database authentication and access is controlled by record and/or field

Audit Scope: Constrains the audit to a specific system, function, or unit, or period of time

- E.g., Scope is constrained to Headquarters for the last year.

Workbook:

Audit Plan

Objective: Determine safety of Web interface

Scope: External penetration test on all company Web pages

Constraints: Must test between 1-4 AM

Approach:

1. Tester has valid session credentials
2. Specific test records are available for attack
3. SQL Injection

Checklist

- The following databases & forms: A, B, C.
- The following security attacks: X, Y, Z.

Signatures: Ellie Smith Pres. Terry Doe CISA

Step 3: Add Detail to Plan

- Translate basic audit objective into specific IS audit objectives
- Identify and select the audit approach to verify and test controls
- Identify individuals to interview
- Obtain departmental policies, standards, procedures, guidelines to review
- Develop audit tools and methodology

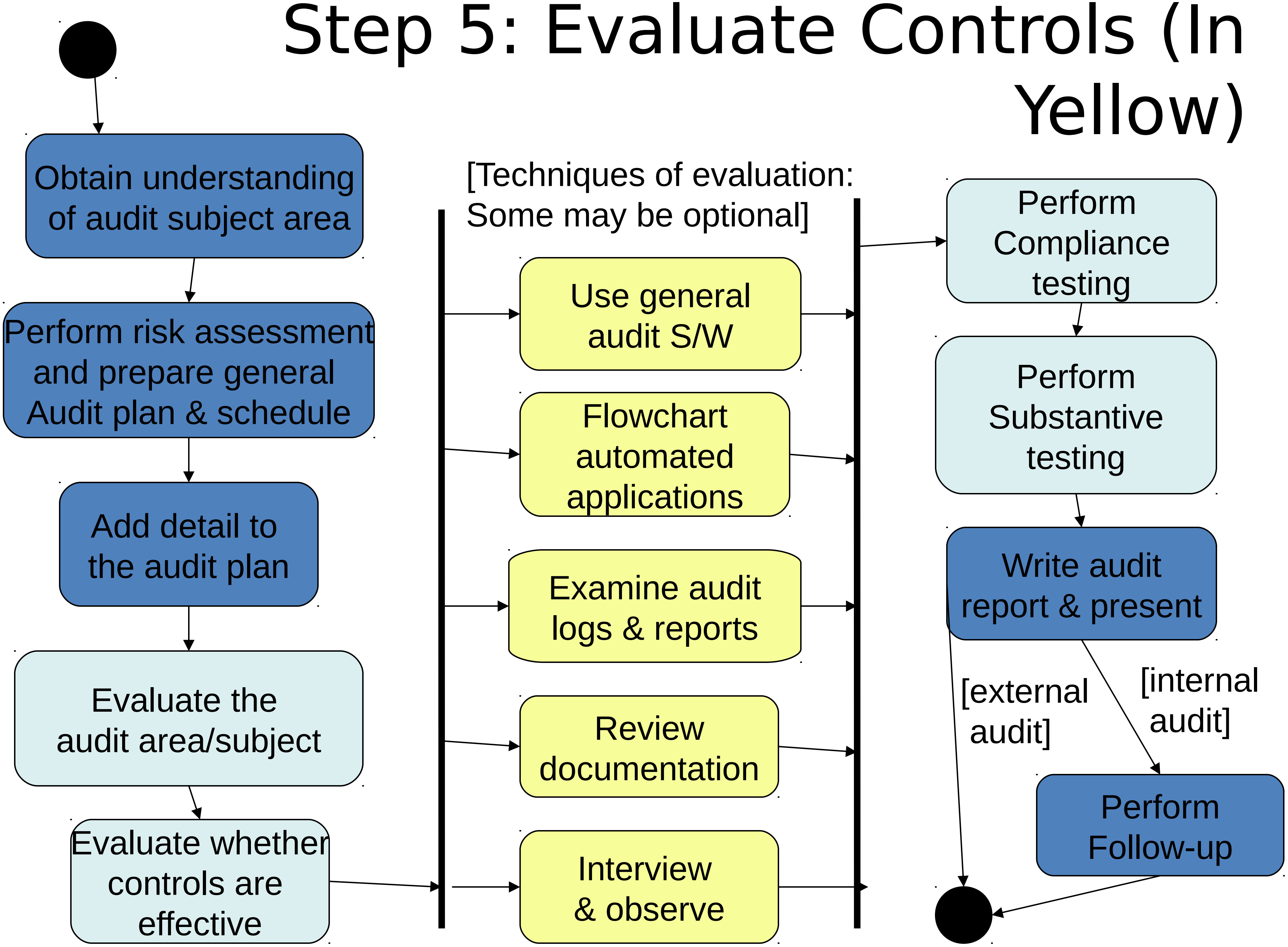
Step 3: Add Detail to Plan
Step 4: Evaluate Audit Area

Tools for the Auditor

ISACA has Standards and Guidelines related to Audit

- Section 2200 General Standards
- Section 2400 Performance Standards
- Section 2600 Reporting Standards
- Section 3000 IT Assurance Guidelines
- Section 3200 Enterprise Topics
- Section 3400 IT Mgmt Processes
- Section 3600 IT Audit and Assurance Processes
- Section 3800 IT Audit and Assurance Mgmt

Step 5: Evaluate Controls (In Yellow)


Obtain understanding of audit subject area
Perform risk assessment and prepare general Audit plan & schedule
Add detail to the audit plan
Evaluate the audit area/subject
Evaluate whether controls are effective
[Techniques of evaluation: Some may be optional]
Use general audit S/W
Flowchart automated applications
Examine audit logs & reports
Review documentation
Interview & observe
Perform Compliance testing
Perform Substantive testing
Write audit report & present
[external audit]
[internal audit]
Perform Follow-up

Step 5: Evaluate Controls

Review IS Organization: Separation of duties

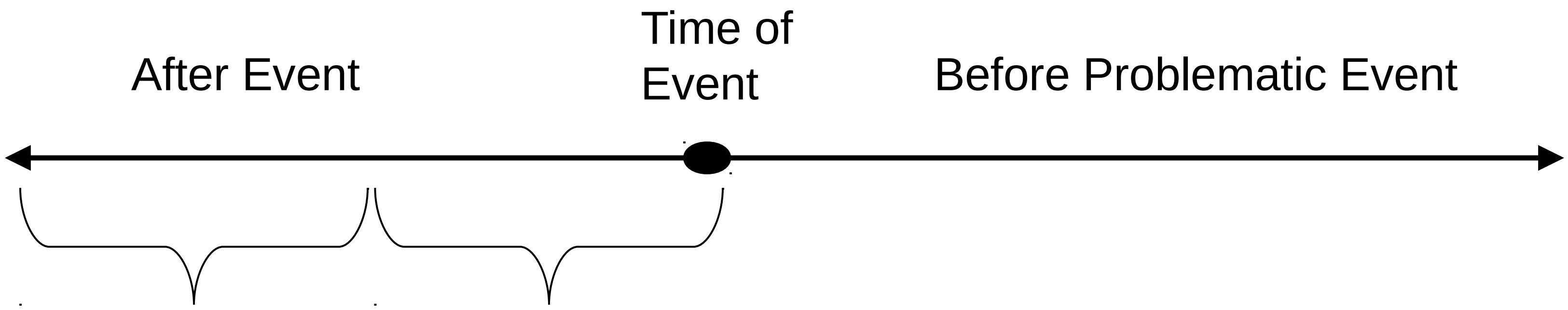
Review IS Policies, Standards, Procedures: Defined, periodically updated

Review IS Documentation: Policy, Procedures, Design, Test, Operations, Contract/SLAs, Security

Interview personnel: Segregation of duties, security awareness, competency

Observe personnel: Document everything in sufficient detail

Evaluate Controls: IT Control Classifications



After Event

Time of Event

Before Problematic Event

Corrective Controls:
Fix problems and prevent future problems
Includes:
Contingency planning
Backup procedures
Reruns

Detective Controls:
Finding fraud when it occurs
Includes:
Hash totals
Check points
Duplicate checking
Error messages
Past-due account reports
Review of activity logs

Preventive Controls*:
Preventing fraud

Includes:
Programmed edit checks
Encryption software
Access control S/W
Well-designed procedures
Physical controls
Employ only qualified personnel

Evaluate Controls: Simple Control Matrix

Error-> Control v	Disk failure	Hack	Fraud	Social Engineer
Access Control			weak	
Authentication		strong		
Firewall		medium		
Physical: locked door		weak		

Compensating Control: A strong control supports a weak one.
Overlapping Control: Two strong controls

Step 6 & 7: Audit Test

Evidence: Audit findings must be based on sufficient and reliable evidence and appropriate interpretation of the evidence

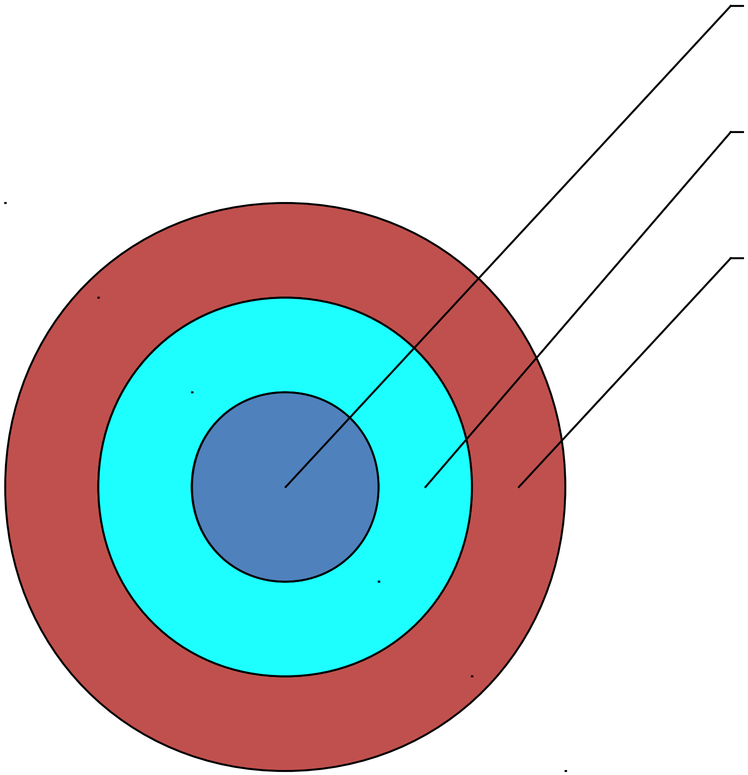
Documentation: The audit work and audit evidence to support conclusions must be fully documented

Supervision: Audit staff is supervised to ensure that audit is professionally completed

Professional Skepticism: The auditor must keep an eye open for irregularities and/or illegal acts, unusual relationships, material misstatements

- when irregularities are encountered, the auditor should:
  - Investigate fully
  - document all communications, tests, evidence, findings
  - report the irregularity to governance body in a timely manner

Substantive vs. Compliance Testing



Substantive Testing: Does the business application work as reqd

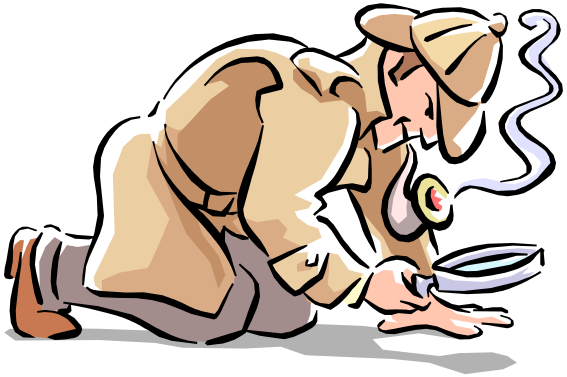
Does Sales Application work?

Compliance Testing: Do the controls work?

Does access control limit access?

Compliance Testing:

Does Authentication require complex passwords?



Test Vocabulary

Compliance Testing:

- Are controls in place and consistently applied?
  - Access control
  - Program change control
  - Procedure documentation
  - Program documentation
  - Software license audits
  - System log reviews
  - Exception follow-ups

Substantive Testing:

- Are transactions processed accurately?
- Are data correct and accurate?
- Double check processing
  - Calculation validation
  - Error checking
  - Operational documentation
- If Compliance results are poor, Substantive testing should increase in type and sample number

Step 6: Compliance Testing

- Control: Is production software controlled?
  - Test: Are production executable files built from production source files?
  - Test: Were proper procedures followed in their release?

- Control: Is Sales DB access constrained to Least Privilege?
  - Test: Are permissions allocated according to documentation?
  - Test: When sample persons access DB, can they access only what is allowed?

Step 7: Substantive Testing

- Audit: Is financial statement section related to sales accurate?
  - Test: Track processing of a sample transactions through the system, performing calculations manually
  - Test: Test error conditions

- Audit: Is tape inventory correct?
  - Test: Search for sample days and verify complete documentation and tape completeness

Sampling

Statistical Sampling:

- N% of all items randomly tested
- Should represent population distribution

Nonstatistical (or Judgment) Sampling:

- Auditor justifies another distribution for sample selection
- Which items are most risky?

Under what conditions do you think one is better?

Generalized Audit Softwa (GAS)

- File Access: Read records & file structures
- File reorganization: Allow sorting, indexing, merging/linking with other files
- Data Selection: Select a set of records
- Statistical functions: Perform sampling, stratification, frequency analysis
- Arithmetic Functions: Perform arithmetic operations on data sets

Step 8: Prepare Audit Report

Identify:

- Organization, recipients, restriction on circulation
- Scope, objectives, period of coverage, nature, timing and extent
- Findings, conclusions, recommendations/follow up, and reservations or qualifications
  - Grouped by materiality or intended recipient
  - Mention faults and constructive corrections
- Evidence to support results (may be separate)
- Overall findings, conclusion, & opinion
- Signed & dated

Workbook:

Audit Report

Objective: Determine safety of Web interface

Scope: External penetration test on all company Web pages

Findings, conclusions, recommendations: The following attacks were successful on the indicated databases. Also listed are the recommended fixes.

Evidence: Screenshots are attached in Appendix A.

Conclusion: Web interface A and B were secure, but Web interface C and D need additional security.

Signed: John Smith, CISA CISSP **Date:** 7/13/2011

Evidence

Forms of Evidence

- Notes from Interviews
- Test Results
- Email or mail correspondence
- Documentation
- Observations

Best Sources

- External: Sources from outside organization
- Qualified: Most knowledgeable
- Objective: Evidence not prone to judgment
- Timing: Should match period under review

Communicating Results

Auditor

2. Report findings material to their interests

Upper Management/Board

1. Reports findings material to their areas; Obtain agreement & course of correction Document agreements & implications of problems where disagreement occurs..

Lower Management

Step 9: Follow-up

- Has management taken appropriate action to fix problems in a timely manner?
- Request and evaluate information on follow-up
  - Management should schedule implementation of correction
  - May be scheduled for convenient time
  - Next audit these follow-ups should be checked

Final IMPORTANT Recommendation

IS Audits can result in system failures, problem

Protect Yourself:

- Get an approval signature for your audit plan before you begin: This is your **Get Out of Jail Card!**
- If you will be impacting the system at all, send an email to all affected and talk to the administrators before starting any tests
- When working with data or devices, be careful not to be the CAUSE of any problems; be careful not to change live data or configurations for test purposes: Work on a copy!
- Preferably have an escort for all that you do

There is one difference between a hacker and auditor:

Permission!!!

Classifications of Audit

Financial Audit: Assure integrity of financial statements

Operational Audit: Evaluate internal controls for a given process or area

Integrated Audit: Includes both Financial and Operational aspects

Forensic Audit: Follows up on fraud/crime

IS Audit: Does IS safeguard data, provide CIA in efficient way?

Administrative Audit: Assess efficiency of a process or organization

Specialized Audit: Example:

- **SAS 70**: Assesses internal controls of a service organization

Computer-Assisted Audit Techniques (CAAT)

- Software tools enable auditor to
  - Access and analyze data in database
  - Perform compliance tests
  - Perform penetration and vulnerability tests
  - Test Application
- May include utility software, debug or scanning software, test data, application trace, expert systems, generalized audit software
- Special use:
  - Referenced in audit plan & report
  - Download sample data and use in read-only mode

CAAT—Computer Assisted Auditing Techniques & Tools

- Query systems, report writers, utilities, computer languages
- Complete files can be read speedily
- Can use parameters that may be altered each time program is run
- Once programs are set up, time savings are significant
- Allows auditor independence

CAAT—Computer Assisted Auditing Techniques & Tools

TYPES OF SOFTWARE

- Automated audit workpapers
- Data Analysis
- Risk assessment
- Scheduling
- Timekeeping
- Flowcharting
- Report generation

CAAT—Computer Assisted Auditing Techniques & Tools

USE IN FRAUD DETECTION & INVESTIGATION

- Terminated employees being paid
- Ghost employees
- Purchases to homes instead of business
- “On-call” pay abuse Unusually high salary increases
- Telephone use abuse
- Travel reimbursement abuse

CAAT—Computer Assisted Auditing Techniques & Tools

USE IN NETWORK SECURITY

- Port scanning tools
- Network intrusion detection
- SANS "Top 20 Network Vulnerabilities"
- Computer Intrusion Response Teams

Control Self-Assessment

- Internal audit system that enhances external audit
- Control monitoring occurs in functional areas
- Includes designing and assessing controls locally, often in workshops
- Benefit: Involves and trains employees, often reducing risk quicker

Emerging Audit Techniques

Automated Work Papers: Automated tools for risk & audit reporting

Integrated Audit: Combines financial and IS audit via team effort

Continuous Audit: Provides audit reports on continuous basis (not just quarterly)