fjdke9

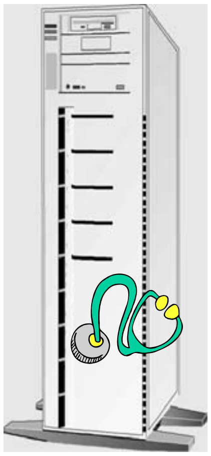
Auditing Computer Security

Supplement to CSH5 Chapter 54
“Security Audits, Standards and Inspections”

Notes by M. E. Kabay, PhD, CISSP-ISSMP
Assoc Prof Information Assurance
School of Business & Management
Norwich University

Topics

- Introduction to Auditing
- EDP System Controls
- Responsibility for Control of EDP
- Auditing Computer Applications
- Reporting Audit Results



Introduction to Auditing

- Controls
- Auditors
- External & Internal Auditors
- EDP Auditors
- Scope of Computer Security
- Security Audits vs Security Assessments
- Psychological Aspects of Audits and Assessments

Controls

- Traditional financial controls
  - ❑Financial records
  - ❑Accuracy – correct representation of reality
  - ❑Integrity – resistance to unauthorized modification or destruction
  - ❑Authenticity – correct attribution of information
- Internal controls
  - ❑Protection of assets
  - ❑Reliability of information

Auditors

- Auditors are independent assessor of internal controls
- Reports to stakeholders
  - ❑Management
  - ❑Regulatory authorities
  - ❑Shareholders
  - ❑Employees
  - ❑Clients
  - ❑Suppliers
  - ❑Public

External & Internal Auditors

- *Internal* auditors report to board of directors
  - ❑Safeguard assets (physical, data, $$)
  - ❑Ensure accuracy and reliability of data
  - ❑Promote operational efficiency
  - ❑Enforce adherence to policies
  - ❑Compliance with regulatory/legal requirements
- *External* auditors hired for completely independent evaluation
  - ❑Potential problems if external auditors see their interests too closely tied to those of management

The Equity Funding Fraud (1)

Public Offering 1964
Earnings ~ $390,000
Revenues ~ $3 Million

By the end of 1972
Earnings > $22 Million
Revenues of 152.6 Million
Assets of $750 Million
Net Worth of $143.4 Million

1973
> Half of 99,052 policies – fake
I.e., > 49,526 policies with an estimated worth of $2 Billion

Of $117 million in loan receivables $62 Million did not exist

(Thanks to G. Will Milor for images and factual details)

The Equity Funding Fraud (2)

- Auditing firm accepted unusual delays in providing factual underpinnings for non-existent insurance policies
  - ❑Executives would create dossiers overnight
- Fees for 1970*
  - ❑Equity Funding - $300,000 / year
  - ❑Next biggest - $75,000 / year
  - ❑Next biggest - $25,000 / year
- ALL other accounts together did not equal half of the yearly revenue from EFCA

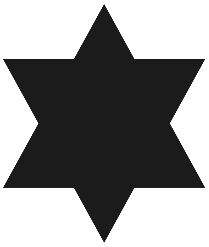
*Thanks to G. Will Milor, MSIA for factual details

EDP Auditors

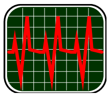
- Early computers used mostly for accounting
- Financial accountants audited computer systems by focusing on output
- With wider applications and greater complexity, new field developed: EDP auditing
- Includes operational controls, programming issues
- Work with development, operations, security personnel

Scope of Computer Security

- Wide range of issues affecting six fundamental aspects of information in *Parkerian Hexad*:
  - ❑Confidentiality
  - ❑Control or possession
  - ❑Integrity
  - ❑Authenticity
  - ❑Availability
  - ❑Utility
- Many aspects of data processing are interesting to EDP auditors



Security Audits vs Security Assessments



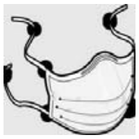
- Distinction often made between *audit* and *assessment*
- Audit determines compliance with stated policies
- Assessment can go beyond policies and assess compliance with industry standards
  - ❑*Best practices*
  - ❑Formal standards such as ISO17799
  - ❑Consultant’s own experience and judgement

Psychological Aspects of Audits and Assessments

- Auditors can be viewed as threats
  - ❑Staff may perceive audit as blame game
  - ❑“Failure” of audit leads to punishment
  - ❑Auditors are “the enemy”
- Work to defuse negative feelings
  - ❑Meet staff at start of audit
  - ❑Encourage cooperation
  - ❑Part of continuous process improvement
  - ❑Not intended to blame or punish individuals
  - ❑Everyone can suggest and benefit by improvements

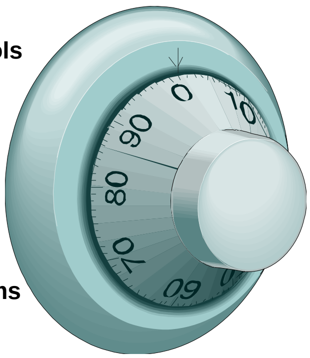
EDP System Controls

- Apply controls to two spheres
  - ❑Overall EDP Controls
  - ❑Individual Application Controls
- Focus on 3 types of controls
  - ❑Preventive
  - ❑Detective
  - ❑Corrective
- Distinguish between types of controls
  - ❑Discretionary
  - ❑Mandatory



Overall EDP Controls

- Separation of Duties
- System Development Controls
- Operations Controls
- Change Control
- Quality Assurance
- Telecommunications
- Program Libraries
- Data Libraries
- Hardware & Software Systems



Separation of Duties

- Make crime more difficult by requiring collusion
- Restrict computer-room access
- Supervise visitors at all times
- Restrict program & file access on need-to-know basis

- Require at least 2 independent approvals for disbursements or operational changes
- Segregate program development team from quality assurance personnel and from operations
- Assign security responsibilities to separate chain of command

System Development Controls

- Use formal system development methodology
- Maintain proper documentation throughout system development
- Integrate quality assurance throughout SDLC
- Integrate security engineering throughout
- Establish rigorous controls for maintenance (change management)
- Establish documented operational procedures

Water Rocket Launcher Flowchart
Turn OFF Abort Valve
Dry Ice Launch?
Yes
No
Pour Dry Ice Pellets in Rocket
Garden Hose
Yes
No
Mount Rocket on top Launcher
Pour Water in Rocket
DO NOT Use Trigger SAFETY
Yes
Dry Ice Launch?
No
DO Use Trigger SAFETY
Turn ON Launcher's Water Valve & Fill Rocket
Yes
Dry Ice Launch?
No
Add Air Pressure
Launch Immediately when Pressurized
Yes
Ready?
No
Abort

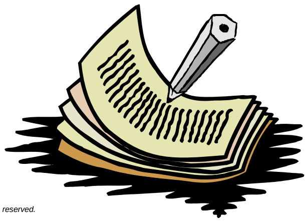
Operations Controls

- Involve operations in SDLC from start
- Develop and document SOP (standard operating procedures)
- Verify adherence to SOP
- Keep logs showing all exceptional conditions
- Verify logs for completeness and accuracy
- Require all production code to pass quality assurance (QA) procedures before implementation
- Proper management of all data media
- Contribute to BCP and DRP (Business Continuity and Disaster Recovery Planning)

http://www.jsc.nasa.gov/history/jsc40/gallery/lores/S65-42424.jpg

Change Control

- Written authorization from users and programming management
- Document all changes
- Document all regression testing
- Complete and up-to-date revisions of all user and operational documentation



Quality Assurance

- Specific people assigned to QA
- QA part of SDLC at all stages
- QA collaborate with operations

Telecommunications

- Control access to reduce risks of unauthorized use
  - ❑Insiders and outsiders
- Separate production from development networks
- Use proper I&A methods
- Encrypt data in flight and at rest
- Monitor datacomm lines for abnormal events
- Prevent misuse of corporate resources (piracy etc.)
- Prevent physical access to network gear

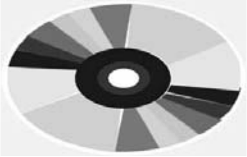
Program and Data Libraries

- Product code to be stored in libraries
  - ❑Only authorized development personnel to make changes for specific reasons
  - ❑Only production personnel to use these libraries
- Databases restricted
  - ❑Access strictly limited by need; e.g., accounting, engineering, personnel…
  - ❑Can further protect using selective *views* of data (only certain rows or columns for specific users)
  - ❑May also encrypt specific rows or columns

http://home.intekom.com/rylan/art/alexandria.jpg

Hardware & Software Systems

- Access to physical computer equipment dangerous
- Operating software must be maintained in pristine condition
  - ❑*Known-good software* used for reinstallation
- Reduce risk of downtime
  - ❑Deliberate attack (sabotage, vandalism, extortion)
  - ❑Accident (oversight, error)



Individual Application Controls

- Inputs
- Processing
- Output Controls

Inputs

- Verify key entry
  - ❑Check digits
  - ❑Preprocessing edits
- Batch controls
- Master file references
- Edit programs

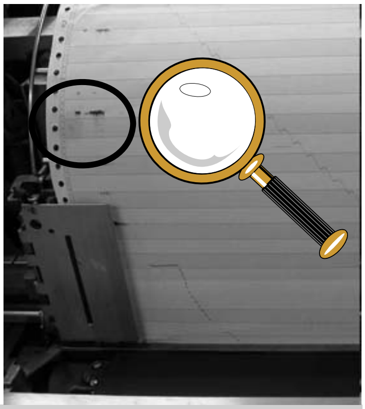
Processing

- *Test-decks* with known outputs
- *Batch or total controls* integrated into data stream
- *Cross-footing tests* compare totals for consistency (e.g., sums of rows vs sums of columns)
- *Application reruns* (with automated comparison of results in 1st and 2nd calculations)

http://tinyurl.com/22ek8q

Output Controls

- Verify quality of all output
  - ❑Files
  - ❑Tapes
  - ❑Disks
  - ❑Paper
- For users, can be single most important metric of quality and service



http://ed-thelen.org/1401Project/1403PaperMovementRGOct05-.jpg

Responsibility for Control of EDP

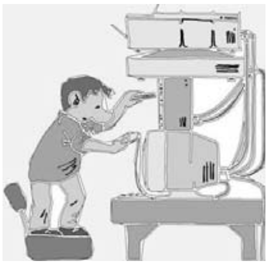
- Senior Management
- EDP Management & Staff
- Auditors

Senior Management

- Create positive attitude towards control and security
- Establish & communicate policies
- Provide adequate funding for monitoring and awareness
- Establish security steering group

EDP Management & Staff

- Assign specific person with responsibility and authority for controls; e.g.,
  - ❑Chief Information Security Officer (CISO)
  - ❑Information Systems Security Officer (ISSO)
  - ❑Data Security Manager . . .
- Define staff functions; e.g.,
  - ❑Data classification
  - ❑Risk assessments
  - ❑Security awareness and training
  - ❑Data collection for cost justification. . .



Auditors

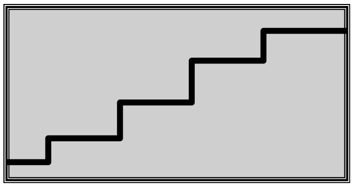
- Internal auditors should not report to the managers whose systems they audit
  - ❑Ideally, should have a Director of Internal Audit who reports to the Board of Directors
  - ❑Same level as other “C” executives (CEO, COO, CFO, CIO, CISO….)
- Collaborate with colleagues to improve controls and security
- Non-adversarial stance more effective than punitive attitude

Auditing Computer Applications

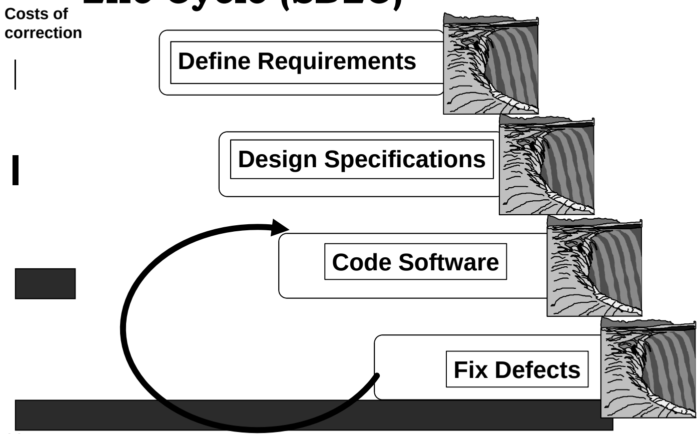
- Audit During Development
- Work Papers
- Data Audit Programs
- Source Code Comparison Programs
- Other File Comparison Programs
- Computer-Assisted Audit Techniques
- Special PC Issues
- Backup & Recovery

Audit During Development

- Work closely with Software Quality Assurance (SQA) personnel
- Strive to identify and help correct flaws before they enter production
- Cost of correction rises by 10x with every stage of the System Development Life Cycle (SDLC)



The System Development Life Cycle (SDLC)

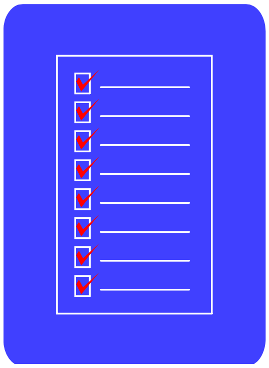


Work Papers

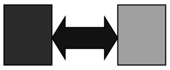
- Detailed *audit trail* of all aspects of the investigation
  - ❑Meetings
  - ❑Reports
  - ❑Documents
  - ❑Correspondence (including e-mail)
  - ❑Checklists
  - ❑Test methods and results
  - ❑Responses to missing controls or data
- Conclude with summary evaluation of adequacy of controls

Data Audit Programs

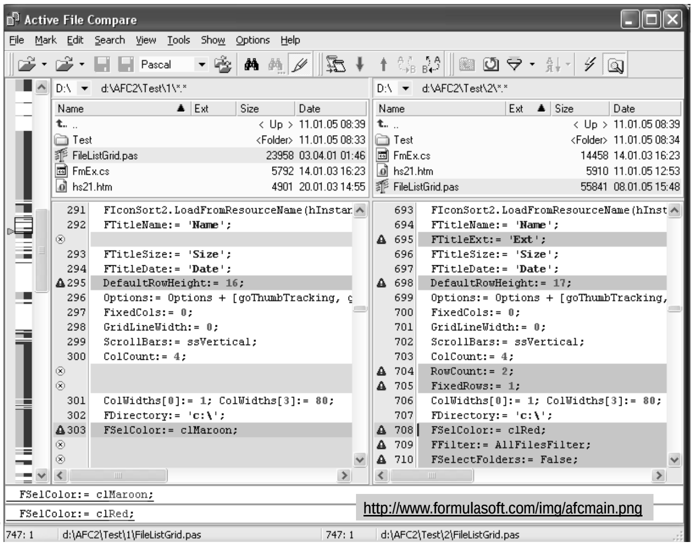
- Special programs for investigating data
- Diagnostic routines for databases
- Verification of backup validity
- Reading & interpreting audit logs
- Auditing software licenses for piracy
- Checking for pornography on workstations
- Random sampling of data
- Repeat calculations
- Check for violation of business rules



Source-Code Comparison Programs (1)



- Track all changes to source code for production programs
- Compare compiled programs with source code ostensibly used to create them
- Especially important for open-source programs
- May not be possible for proprietary COTS software (no source code available without special contractual arrangements -- difficult)
- See next page for example of comparison tool



D:\ d:\AFC2\Test\1\*.*

Name	Ext	Size	Date
..		< Up >	11.01.05 08:39
Test		<Folder>	11.01.05 08:33
FileListGrid.pas		23958	03.04.01 01:46
FmEx.cs		5792	14.01.03 16:23
hs21.htm		4901	20.01.03 14:55

D:\ d:\AFC2\Test\2\*.*

Name	Ext	Size	Date
..		< Up >	11.01.05 08:39
Test		<Folder>	11.01.05 08:34
FmEx.cs		14458	14.01.03 16:23
hs21.htm		5910	11.01.05 12:53
FileListGrid.pas		55841	08.01.05 15:48

```
FIconSort2.LoadFromResourceName(hInstar
FTitleName:= 'Name';

FTitleSize:= 'Size';
FTitleDate:= 'Date';
DefaultRowHeight:= 16;
Options:= Options + [goThumbTracking, g
FixedCols:= 0;
GridLineWidth:= 0;
ScrollBars:= ssVertical;
ColCount:= 4;


ColWidths[0]:= 1; ColWidths[3]:= 80;
FDirectory:= 'c:\';
FSelColor:= clMaroon;
```

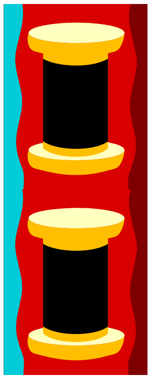
```
FIconSort2.LoadFromResourceName(hInst
FTitleName:= 'Name';
FTitleExt:= 'Ext';
FTitleSize:= 'Size';
FTitleDate:= 'Date';
DefaultRowHeight:= 17;
Options:= Options + [goThumbTracking,
FixedCols:= 0;
GridLineWidth:= 0;
ScrollBars:= ssVertical;
ColCount:= 4;
RowCount:= 2;
FixedRows:= 1;
ColWidths[0]:= 1; ColWidths[3]:= 80;
FDirectory:= 'c:\';
FSelColor:= clRed;
FFilter:= AllFilesFilter;
FSelectFolders:= False;
```

```
FSelColor:= clMaroon;
FSelColor:= clRed;
```

```
747: 1    d:\AFC2\Test\1\FileListGrid.pas    747: 1    d:\AFC2\Test\2\FileListGrid.pas
```

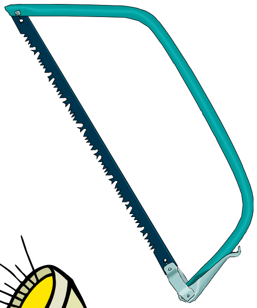
http://www.formulasoft.com/img/afcmain.png

Other File-Comparison Programs

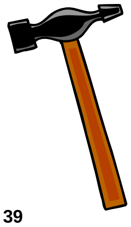


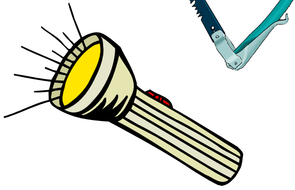
- Byte-for-byte comparison possible
- Especially useful when comparing output of test run against production run
  - ❑Write output to *spool files* on disk
  - ❑Compare spool files
  - ❑Much used in system acceptance testing (QA)
- Auditors can order a duplication of a production run and compare results to previous output

Computer-Assisted Audit Techniques



- Wide range of tools available; e.g.,
  - ❑Generalized audit software
  - ❑Embedded audit data collection
  - ❑System utilities





Special PC Issues

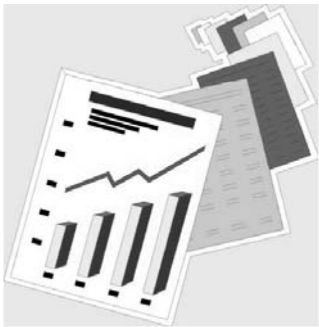
- PCs typically have fewer security controls
- Can serve as vector for release of confidential data
- Some people develop *ad hoc* methods on their PCs that insensibly become production methods – but have no documentation or controls
- Be on guard against *unauthorized encryption* of corporate data
- Unauthorized use of PCs for disallowed functions (gambling, pornography, harassment, piracy, etc.)

Backup & Recovery

- All systems should have adequate BU and recovery in place
- Verify that these methods are actually *used*
- Verify that BU media are readable
  - ❑Some operators disable verification to “save time”
  - ❑Can result in disasters
- Ensure that contingency plans are
  - ❑In place
  - ❑Tested
  - ❑Updated

Reporting Audit Results

- Executive Summary (1 page)
- Objectives
- Methods
- Results
- Analysis
- Discussion and Recommendations
- Graphical representation of results often useful (see following diagrams)



Summary of Status 1 Year Ago

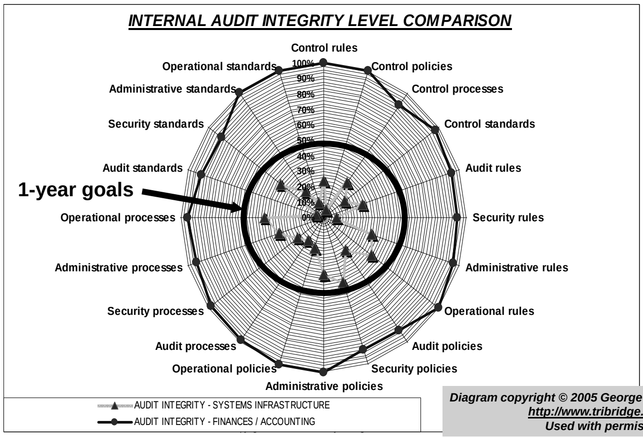
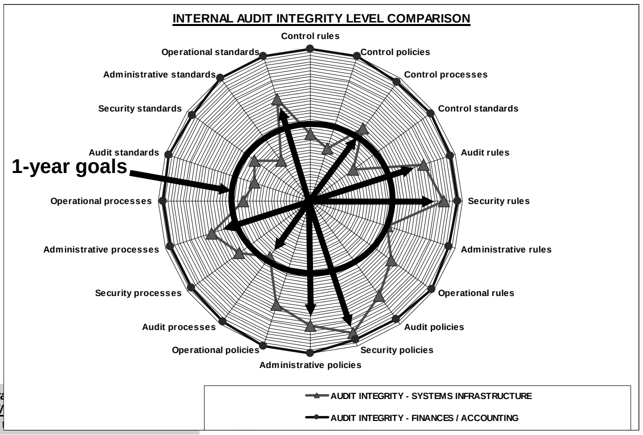


Diagram copyright © 2005 George Mills
http://www.tribridge.com
Used with permission.

Summary of Current Status



Diagra
http://
Used

Goals for 6 Months From Now

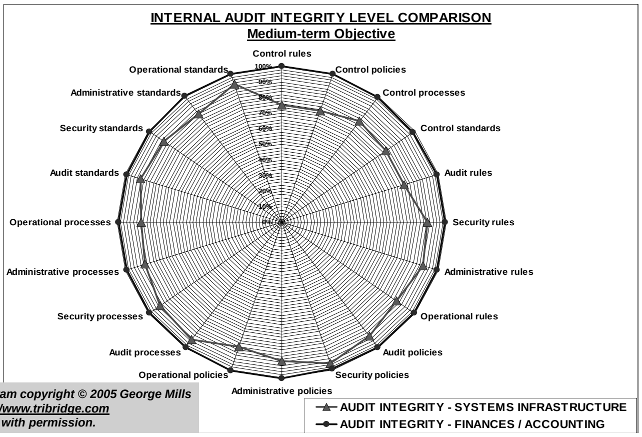


Diagram copyright © 2005 George Mills
http://www.tribridge.com
Used with permission.

Long-Term Goals

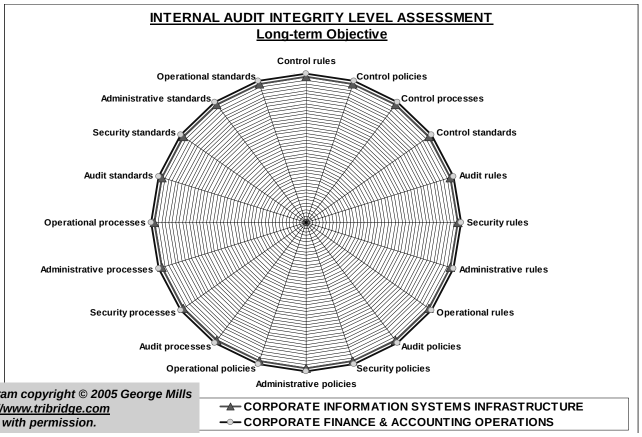


Diagram copyright © 2005 George Mills
http://www.tribridge.com
Used with permission.

Review Questions (1)

1. What do you think are the advantages and disadvantages of internal vs external auditors?
2. Explain why separation of duties is important for security and give examples of what auditors look for in evaluating the quality of controls involving separation of duty.
3. What kinds of questions would an auditor ask about the system development practices in an organization being audited?
4. What does an auditor look for in program revision controls?
5. If you were doing an audit, how would you tell if telecommunications were being properly controlled?

Review Questions (2)

6. Make up an example to illustrate each of the four methods of input controls described in the text.
7. Why should an audit team keep careful written records of their methods and findings? Who cares about such things?
8. What are key elements an auditor looks for in operations security?
9. How do auditors verify that data processing is being carried out properly by application programs?
10. What are some of the special considerations auditors look for in evaluating PC policies and management?
11. Where do backups fit in the audit scheme?