IS AUDIT

Procedures of IS Audit

IS Audit
ACKNOWLEDGMENTS

Material is sourced from:

CISA® Review Manual 2011, ©2010, ISACA. All rights reserved. Used by permission.

Author: Susan J Lincke, PhD
Univ. of Wisconsin-Parkside

ReviewersContributors: Todd Burri, Kahili Cheng

Funded by National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and/or source(s) and do not necessarily reflect the views of the National Science Foundation.
OBJECTIVES

Students should be able to:

Define audit risk: inherent risk, control risk, detection risk, overall audit risk

Describe substantive test and compliance test

Define control types: compensation, overlapping, preventive, detective, corrective

Describe sampling types: statistical, nonstatistical, variable, attribute, stop-or – go

Define audit types: financial, operational, administrative, IS, integrated, forensic

Describe CAAT, GAS, Control Self-Assessment, Continuous Audit

Develop a simple audit plan and audit report (Exercise: related to logs)
CISA DEFINITION FOR AUDIT

“Systematic process by which a qualified, competent, independent team or person objectively obtains and evaluates evidence regarding assertions about a process for the purpose of forming an opinion about and reporting on the degree to which the assertion is implemented.”
AUDITOR QUALIFICATIONS

Independent:

**Professional Independence:** Auditor acts independent of group being audited
- No friendships, dating, suggestive language, parties, lunches

**Organizational Independence:** Auditor and his/her organization has no special interest in the audited organization

AdHERE to Professional Ethics Standard
- ISACA standard and professional care

Professional Competence
- Has skills/knowledge to complete task
- Continued professional training/education
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?
## Audit Planning Table

<table>
<thead>
<tr>
<th>Audit Area</th>
<th>Time-frame</th>
<th>Date of Last Test</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies &amp; Procedures for Registration, Advising</td>
<td>1Q</td>
<td>Never</td>
<td>Internal Auditor</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>2Q</td>
<td>2010</td>
<td>CIO, Security Consultant</td>
</tr>
<tr>
<td>FERPA: Personnel interviews</td>
<td>3Q</td>
<td>Never</td>
<td>Internal Auditor</td>
</tr>
<tr>
<td>IT: Penetration Test</td>
<td>4Q</td>
<td>2011</td>
<td>CIO, Security Consultant</td>
</tr>
</tbody>
</table>
**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**

1. **Plan audit & gather info.**
2. **Review internal control**
3. **Perform compliance & substantive tests**
4. **Prepare & present report**
AUDIT ENGAGEMENT PROCEDURE

1. Obtain understanding of audit subject area
2. Perform risk assessment
   Prepare audit engagement plan
3. Review plan with auditee
4. Evaluate whether control design is effective
5. Use general audit s/w
   Run tests
6. Flowchart automated applications
7. Examine audit logs & reports
8. Review documentation
9. Interview & observe
10. Evaluate Compliance Test results
11. Evaluate Substantive Test results
12. Write audit report & present
13. Perform Follow-up

[Techniques of evaluation: Some may be optional]

[external audit] [internal audit]
STEP 1A: 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
AUDIT ENGAGEMENT 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 is safe against data breaches, due to inappropriate authentication, access control, or hacking

**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.
STEP 1B: 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

What Inherent, Control & Detection Risks exist on the IT side?
## Audit Engagement Risk Analysis

### Inherent Risks: (Risks organization is predisposed to)

**Data Breach:** Student grades, disabilities (FERPA), student health (HIPAA), student/employee financial acct, payment card info. (PCI DSS), SSN and passport numbers (State Breach). Students agree to publish contact info. annually (FERPA).

**Hacking:** University is an open system, with no limitations on installed software and BYOD devices. Student homework must be protected.

### Control Risks: (Risk that a control has vulnerability(s))

**Insufficient Firewall/IPS Restrictions:** While much of the university network is open, critical databases must be in a secure zone with a high level of restrictive access.

### Detection Risk: (Risks of auditor not detecting a problem)

**Hacker within Confidential Zone:** This audit may not detect an infiltrated Confidential Zone or critical vulnerability.
STEP 1C: PREPARE AUDIT ENGAGEMENT PLAN

Develop risk-based approach

Include audit objectives, scope, timing, required resources

Comply with applicable law

Develop audit program and procedures
STEP 1C: ADD DETAIL TO PLAN

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

Source: ITAF™, ©2011, ISACA. All rights reserved. Used by permission.
STEP 1C: 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
**Objective:** Determine safety of Web interface

**Scope:** Penetration test on Student-accessed databases.

**Constraints:** Must perform hacking tests between 1-6 AM

**Compliance & Criteria:** State Breach Not. Law, FERPA, PCI DSS

**Approach:**
1. Tester has valid session credentials ('student' with records)
2. Test using manual and automated web testing tools

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

**Signatures:** Ellie Smith CISO    Terry Doe CISA
**STEP 2: EVALUATE CONTROLS:**

**IT CONTROL CLASSIFICATIONS**

<table>
<thead>
<tr>
<th>Corrective Controls:</th>
<th>Detective Controls:</th>
<th>Preventive Controls*:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fix problems and prevent future problems</td>
<td>Finding fraud when it occurs</td>
<td>Preventing fraud</td>
</tr>
<tr>
<td>Includes: Contingency planning</td>
<td>Includes: Hash totals Check points Duplicate checking Error messages Past-due account reports Review of activity logs</td>
<td>Includes:</td>
</tr>
<tr>
<td>Backup procedures Reruns</td>
<td></td>
<td>Programmed edit checks Encryption software Access control S/W Well-designed procedures Physical controls Employ only qualified personnel</td>
</tr>
</tbody>
</table>
## STEP 2: EVALUATE CONTROLS: SIMPLE CONTROL MATRIX

<table>
<thead>
<tr>
<th>Prob-&gt;Control v</th>
<th>Disk Failure</th>
<th>Power Failure</th>
<th>Data Breach</th>
<th>Fraud</th>
<th>Hack</th>
<th>Malware</th>
<th>Social Engineer</th>
<th>Missing Equip.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authenticaion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logs/Alarms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strong policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vuln Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **p**: Present
- **pp**: Present in Pair
- **ppp**: Present in Triple
- **cc**: Controlled
- **dd**: Documented

*Note: The table entries indicate the presence or absence of controls for each identified threat.*
**STEP 3: PERFORM TESTS**

1. Obtain understanding of audit subject area
2. Perform risk assessment
3. Prepare audit engagement plan
4. Review plan with auditee
5. Evaluate whether control design is effective

**[Techniques of evaluation: Some may be optional]**

- Use general audit s/w
- Run tests
- Flowchart automated applications
- Examine audit logs & reports
- Review documentation
- Interview & observe

6.Evaluate Compliances Test results
7. Evaluate Substantive Test results
8. Write audit report & present
9. Perform Follow-up

[external audit] [internal audit]
STEP 3: PERFORM TESTS

**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
STEP 3: PERFORM TESTS

**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
Compliance Testing:
Does Authentication require complex passwords?

Compliance Testing:
Does access control limit access?

Substantive Testing:
Does Sales Application work?
STEP 3: 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 3A: 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 3B: 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

Variable Sampling: How accurate is the sample population in matching the full population?
- Determine appropriateness of sampling: (e.g., $, weight, amount):
  Sample average $24.50, Real average: $26.99

Nonstatistical (or Judgment) Sampling:
Auditor justifies another distribution for sample selection
Which items are most risky?
DIFFERENCE ESTIMATION SAMPLING

Population:
- Population Mean (Average)
- Population Standard Deviation

Sample:
- Sample Mean
- Sample Std. Dev

Precision: Acceptable range between Sample and Population

Confidence Coefficient or Level: The probability that the sample represents the actual population

Level of Risk = 1 – Confidence Level
VARIABLE SAMPLING

Group statistical distribution is known?

Yes

- Samples selected from groups?
  - Yes
    - Stratified Mean per Unit
  - No
    - Difference Estimation
      - Difference between audited values and real population is noted

No

- Unstratified Mean per Unit
  - Group distribution is estimated from sample testing
SAMPLING

**Tolerable Error Rate:** The maximum allowable error rate (e.g., inappropriately documented changes)

**NonStatistical Sampling** includes:

**Discovery Sampling:** A minimal testing model used when the expected occurrence rate is extremely low (e.g., find fraud, break laws)

**Stop-or-Go Sampling:** If the first 20 have zero errors, then stop. Else if the first 100 have < 10 errors, stop. Else...

**Attribute Sampling:** How many of X have Y attribute? E.g. How many changes are appropriately documented?
GENERALIZED AUDIT SOFTWARE (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 4: 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
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
WORKBOOK:
AUDIT REPORT

2014 Audit Report for
Einstein University’s Student DB Web Interface

**Objective:** Determine safety of Web interface

**Scope:** External penetration test on all company Web pages

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

**Detailed Findings and Recommendations:** The following attacks were successful on the indicated databases. Also listed are the recommended fixes.

**Evidence:** Screenshots are attached in Appendix A.

**Signed:** John Smith, CISA CISSP    **Date:** 7/13/2014
COMMUNICATING RESULTS

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

2. Report findings material to their interests

Auditor

Upper Management/Board

Lower Management
STEP 4B: 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
IS Audits can result in system failures, problems, etc.

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**: Evaluates IS safeguards for data in providing CIA efficiently

**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
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, operational, and/or IS audit via team effort

**Continuous Audit:** Provides audit reports on continuous basis (weekly, daily, hourly)
Wrong Way:

You: I developed an audit plan for Help-The-Community

Interviewer: What specifically did you do?

You: We tried to break into their wireless network.

Interviewer: What did you find?

You: They had no security. They were hopelessly non-technical. Their password was ‘HelpTheCommunity’, and transmissions were unencrypted. I could read everything…

What is wrong with this dialogue?
SERVICE LEARNING COMPONENT: NON-DISCLOSURE AGREEMENT

Right Way:

You: I developed an audit plan for Help-The-Community

Interviewer: What specifically did you do?

You: We did a penetration test. However, I signed a non-disclosure agreement, so I am not at liberty to say specifically what we did or found.

Interviewer: Were you successful in breaking in?

You: I can’t say. However, if you would like to contact my community partner as a reference, here is her contact information...
The PRIMARY purpose of generalized audit software (GAS) is to:

1. Find fraudulent transactions
2. Determine sample mean compared to population mean
3. Extract data for a Substantive Test
4. Organize an audit report
A Compensating Control is defined as

1. Two strong controls address the same fault
2. A fault is addressed by a weak control and strong control in another area
3. A control addresses a specific problem
4. A control that fixes the problem after it is detected
An IS auditor should plan their audit approach based upon:

1. Materiality
2. Management recommendations
3. ISACA recommendations
4. Risk
A Hash Total is maintained on each batch file to ensure no transactions are lost. This is an example of a

1. Preventive Control
2. Detective Control
3. Compensating Control
4. Corrective Control
The FIRST step that an auditor should take is:

1. Prepare the Audit Objectives and Scope
2. Learn about the organization
3. Study ISACA audit recommendations for the functional area
4. Perform an IT risk assessment
An audit that considers how financial information is generated from both a business process and IS handling side is known as:

1. Financial audit
2. Operational audit
3. Administrative audit
4. Integrated audit
An auditor over-tests (tests a greater percent than actually exist) samples that are expected to be most risky

1. Variable Sampling
2. Attribute Sampling
3. Statistical Sampling
4. Non-statistical Sampling
The possibility that a router does not catch spoofed IP addresses is known as a

1. Inherent risk
2. Control risk
3. Detection risk
4. External risk
Testing a firewall to ensure that it only permits web traffic into the DMZ is known as

1. Compliance Test
2. Substantive Test
3. Detection Test
4. Preventive Test
An inherent risk for a school would be:

1. Students trying to hack into the system to change grades
2. A firewall does not catch spoofed IP addresses
3. An audit does not find fraud which actually exists
4. People do not change their passwords regularly
<table>
<thead>
<tr>
<th>Slide #</th>
<th>Slide Title</th>
<th>Source of Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>IS Audit Definition</td>
<td>CISA: page 51</td>
</tr>
<tr>
<td>9</td>
<td>Extended Audit Procedure</td>
<td>CISA: page 52</td>
</tr>
<tr>
<td>11</td>
<td>Step 2: Perform Risk Assessment</td>
<td>CISA: page 54, 55, 365</td>
</tr>
<tr>
<td>13</td>
<td>Audit Plan Vocabulary</td>
<td>CISA: page 53</td>
</tr>
<tr>
<td>16</td>
<td>Step 3: Add details to Plan Step 4: Evaluate Audit Area</td>
<td>CISA: page 42 – 46</td>
</tr>
<tr>
<td>17</td>
<td>Step 5: Evaluate Controls (In Yellow)</td>
<td>CISA: page 52</td>
</tr>
<tr>
<td>18</td>
<td>Step 5: Evaluate Controls</td>
<td>CISA: page 58, 59</td>
</tr>
<tr>
<td>19</td>
<td>Evaluate Controls: IT Control Classifications</td>
<td>CISA: page 49 Exhibit 1.4</td>
</tr>
<tr>
<td>21</td>
<td>Step 6 &amp; 7: Audit Test</td>
<td>CISA: page 58, 65</td>
</tr>
<tr>
<td>22</td>
<td>Substantive vs. Compliance Testing</td>
<td>CISA: page 57</td>
</tr>
<tr>
<td>23</td>
<td>Test Vocabulary</td>
<td>CISA: page 57</td>
</tr>
<tr>
<td>24</td>
<td>Step 6: Compliance Testing</td>
<td>CISA: page 57</td>
</tr>
<tr>
<td>25</td>
<td>Step 7: Substantive Testing</td>
<td>CISA: page 57</td>
</tr>
<tr>
<td>26</td>
<td>Sampling</td>
<td>CISA: page 60</td>
</tr>
<tr>
<td>27</td>
<td>Difference Estimation Sampling</td>
<td>CISA: page 60, 61</td>
</tr>
<tr>
<td>28</td>
<td>Sampling</td>
<td>CISA: page 60</td>
</tr>
<tr>
<td>29</td>
<td>Variable Sampling</td>
<td>CISA: page 60</td>
</tr>
<tr>
<td>30</td>
<td>Generalized Audit Software (GAS)</td>
<td>CISA: page 62</td>
</tr>
<tr>
<td>31</td>
<td>Step 8: Prepare Audit Report</td>
<td>CISA: page 53 Exhibit 1.5</td>
</tr>
<tr>
<td>37</td>
<td>Classifications of Audit</td>
<td>CISA: page 51, 52</td>
</tr>
<tr>
<td>38</td>
<td>Computer – Assisted Audit Techniques (CAAT)</td>
<td>CISA: page 61 -63</td>
</tr>
<tr>
<td>39</td>
<td>Control Self-Assessment</td>
<td>CISA: page 65, 66</td>
</tr>
<tr>
<td>40</td>
<td>Emerging Audit Techniques</td>
<td>CISA: page 68 -70</td>
</tr>
</tbody>
</table>