Global Information Assurance Certification Paper

A Generalized Application Security Audit Program For Any Computing Platform With Comments

Laura Sioma

December 6, 2000

Introduction

Computer systems contain weaknesses that can pose risks to a company. Weaknesses can occur in hardware architecture, operating system configuration, application design and implementation, and operations. According to the CISA Technical Review Manual, risks may be defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of/or damage to the assets." From the Management perspective, a risk may also be defined as anything "that could prevent an organization from meeting its objectives," per the IIA Operational Auditing Training Manual. Risks may include the possibility of damaged equipment, incorrect calculations, data accessed by unauthorized people, lost data, misuse of the system, and disrupted business operations.

Information Systems Auditors analyze computer systems and operations to ensure that proper controls are in place to minimize the risks. They assess computer systems by evaluating the three E's - Efficiency, Effectiveness, and Economy. Efficiency is smooth performance of a computer system as a whole. Effectiveness is satisfaction of business requirements by the system. Economy is functioning of the system using the optimal resource level.

As stated in the IIA Operational Auditing Training Manual, a full audit process consists of the following four phases:

1) Planning,
2) Examining and Evaluating Information,
3) Communicating Results, and
4) Following-Up.

Planning consists of collecting general background information, assessing business risk, determining the focus of an audit, developing an audit program, and distributing a scope memo. Examining and Evaluating Information is performing data gathering, including interviews, and analyzing the data. Communicating Results is sharing findings and recommendations with the appropriate Managers and technical staff both in-person and via a formal, written audit report. A Management Response Memo is received which includes a formal action plan corresponding to each recommendation accepted and/or an explanation of why recommendation(s) will not be followed. Follow-up is a verification of whether suggested improvements have been implemented.

An audit program is a step-by-step set of audit procedures and instructions that Auditors use to perform the Examining and Evaluating phase of the audit process. Most audit programs are written for a specific application on a given platform. The audit program below is generalized, so it applies to a broader set of applications and platforms.

This paper presents major commonalities among applications that I have reviewed in my role as a Senior Information Systems Auditor. The steps of the following audit program are numbered for ease of use. The concepts presented in this paper have been tested during actual Internal audits conducted in my current position.

I. Audit Objectives

The Auditor must choose the areas on which to focus during a given audit. Typical areas are:

- To understand how the application is used within a business process,
- To evaluate the appropriateness of the computing platform used,
- To evaluate system and application security,
- To evaluate the reliability and usability of the application,
- To evaluate the integrity of interfaces,
- To review routine operations, and
- To evaluate the adequacy of the Business Recovery Plan and the Business Continuity Plan as it applies to the given application.

The Auditor makes his/her choice of objectives based upon 1) the perceived risks associated with the application, 2) the people resources assigned to the project, and 3) the time allotted to the project. At a minimum, application security is reviewed to ensure that only authorized personnel can access the application.

Note that the Business Recovery Plan, also known as the Disaster Recovery Plan, details the recovery of Information Technology (I/T) systems while the Business Continuity Plan is concerned with recovery of business operations.

II. Preparations

Information can be gathered before the Auditor conducts the first interview with an Auditee. Prior to field work, the Auditor can:

- Identify key personnel associated with the application, such as the data owner, the data custodian, the Security Administrator, key technical support people, and typical business users;
- Identify the userbase of interest;
- Gather the appropriate organizational charts;
- Arrange for limited access to the application and application security for the length of the audit; and
- Review the prior audit report and workpapers.

The Auditor is interested in contact information 1) so data is gathered from the employees closest to the application and 2) for the purpose of evaluating “need to know based on job function” and segregation of duties during the upcoming application security evaluation. “Need to know based on job function” refers to a security policy that a user should only have access to production data required to perform his/her job, without having excess privileges. Segregation of Duties is the assurance that employees’ roles and responsibilities do not allow for a conflict of interest.

Depending upon the sensitivity of the data processed within the application, the Auditor may obtain security privileges that allow him/her 1) to verify information obtained from the Security Administrator and/or other Auditees and 2) to personally test and analyze security privileges. **Two important notes of caution: 1) Only test security when you have permission and knowledge to do so. Get the permission in writing. 2) Do not change production data.**

III. Process

An application needs to be reviewed in the context of the business process that it supports. It is helpful for the Auditor to understand the types of transactions processed, key data elements, and the sensitivity of the data. The Auditor may choose to review:

- An overview of the business process;
- The purpose of the application as it relates to the business process;
- The types of business transactions processed by the application; and
- The list of business users who depend upon the application.

The Auditor may request a demonstration of the application to obtain an overall understanding of the business process and how the software supports it. The Auditor may choose a sample of production data and trace it through the process from beginning to end to test for data integrity. Data integrity is the assurance that data is accurate and available. A data integrity test assures that the program logic is working correctly, generating the expected results.

IV. System Controls

The Auditor will review security controls to the application itself by reviewing any of the following:

- The architecture diagram;
- Security to the platform;
- Security to application software files and its corresponding security files and production data files; and
- The list of high privileged users who can update application software.

Quality Application Security Administration is useless if back doors are open at the system level, therefore the Auditor will verify that system controls exist and are strong.

V. Hardware Issues

Software must run on compatible hardware. The Auditor:

- Will identify the computing platform(s) used by the application, including the platform that supports the user interface and platform(s) that support any source and target applications.
- May review whether the platform is the appropriate model and version for the application; and
- May review peripherals used by the application.

The Auditor is interested in hardware issues, so he/she can evaluate whether the hardware is appropriate for the functioning of the application and whether it allows for performance that satisfies business requirements. If the Auditor is not knowledgeable about equipment types, technical support people may be consulted.

VI. Application Security

This audit program assumes that the application is menu based. To evaluate application security, the Auditor must review each item listed below.

- Review Security Administration policies and procedures that apply to the application. Ensure that the procedures address Add/Change/Delete security maintenance.
- Identify the important menus used in the application, including security menus.
- Determine if each menu is adequately restricted to users who have a "need to know, based on job function."
- Review a report of high privileged users.
- Verify that application users are active employees.
- Review the availability of logs and reports.
- Review the security associated with the user interface, if it is on another platform.
- Review the security associated with the transmission of data between platforms, if the application and its interfaces cross platforms.
- Review change control procedures for the application.

Policies and procedures must be written documents approved by Management.

As stated above, users should have just enough security privileges to perform their job. There is a delicate balance to achieving this goal. Verification of security by job function 1) is a test that users can only reach authorized data and 2) is a check for Segregation of Duties.

VII. Reliability and Usability

The Auditor may verify the reliability and usability of the application by considering the following issues:

- The reliability statistics of the application;
- The results of data integrity tests;
- Whether user interfaces are friendly;
- The level of user training provided; and
- The technical support process.

These issues must be satisfied in order for the application to be a success. That is, an application must meet the customers' needs for them to use it on a regular basis and to provide full benefit to the business process.

VIII.Interfaces

Some applications are standalone applications while others have multiple feed systems and target systems. In order to fully evaluate an application, an Auditor may:

- Identify all interfaces with the application;
- Identify which interface(s) is/are critical to the business process; and
- Test the critical interface(s).

This step requires a great deal of judgement based on the Auditor's experience and understanding of the business process. The Auditees can be extremely helpful in choosing which interface is critical to business operations. Evaluation of interfaces is generally done for data integrity purposes.

IX. Operations

Controls should exist to handle routine processing and to address emergency situations. Auditors may assess the following types of operational issues in order to ensure continuity of service to application users:

- Review operational procedures;
- Review troubleshooting procedures;
- Determine if there is adequate technical support;
- Review the adequacy of technical documentation;
- Determine if adequate back-ups exist;
- Review the Business Recovery Plan as it pertains to the application and the platforms on which the application resides; and
- Review the Business Continuity Plan related to the application.

Inadequate technical support, back-ups, and emergency plans could cause delays in system performance and recovery. A lack of back-ups could make a system unrecoverable.

X. Issues

Application specific issues arise during most application security audits. Issues may include:

- Vendor issues;
- Version issues for purchased packages;
- Future plans for replacement of the application;
- Others as identified by the Auditees; or
- Related topics that require further review which are outside the scope of the current audit.

These miscellaneous issues are addressed immediately if they are critical and if time permits. Related issues identified during the audit may become future audits.

XI. Analyses

The Auditor analyzes data gathered thus far, and discusses any open issues with the appropriate contact people. Findings are identified and recommendations are made. Critical findings are resolved immediately, if possible.

Summary

Information Systems Auditors use Audit Programs during the formal audit process. The above generalized application security audit program is a tool that can help an Auditor to review an application in a logical, systematic way. Security Administrators can use the above audit program to identify security controls that should be designed into new applications.

References

Albert, Eric. Computer Application Controls: Review Guide and Audit Program. 02/24/00. URL: http://www.auditnet.org/ (2000).

Hickman, James R. Practical IT Auditing. Boston, MA and New York, New York. Warren, Gorham & Lamont, RIA Group, 1996.

Horton, Thomas R., LeGrand, Charles H., Murray, William H., Ozier, Willis J., and Parker, Donn B. Managing Information Security Risks - Part 1. 08/15/00. URL: http://www.itaudit.org/ (2000).

Operational Auditing: Attendee Workbook. The Institute of Internal Auditors, Inc., 1999. URL: http://www.theiia.org/ (2000).

Pathak, Dr. J. P. IT Audit Approach, Internal Controls, and Audit Decisions of an IT Auditor - Part 1. 06/15/00. URL: http://www.itaudit.org/ (2000).

Pathak, Dr. J. P. IT Audit Approach, Internal Controls, and Audit Decisions of an IT Auditor - Part 2. 08/01/00. URL: http://www.itaudit.org/ (2000).

Sobol, Michael I. IS Auditing for Systems Professionals. Framingham, MA. MIS Training Institute, 1997. URL: http://www.misti.com/ (2000).

Williams, Paul and Darlington, Robert. 2001 CISA Review Technical Information Manual. Rolling Meadows, Illinois. Information Systems Audit and Control Association, Inc., 2000. URL: http://www.isaca.org/ (2000).