Why an

Automated Vulnerability Assessment is not Enough

For the last few years, a concept has grown within the Information Technology (IT) field, that conducting an automated vulnerability assessment, and maybe followed a penetration test is enough to determine and validate vulnerabilities within an information system (IS), thus considering these processes as a full security assessment, within the following lines we will explain the process of an IS Audit and why it is important to be performed side by side with vulnerability assessment and penetration testing.

Although IS audit usually depends upon certain checklist, but it incorporates the use of various systems' reports, user interface, and sometimes, with respect to the experience of the auditor, upon the business logic and the need-to-know principle.

An assessment including only automated vulnerability assessment and penetration testing can detect weak passwords but can't inform us whether the account holder needs the rights she currently has or not, it can detect un-patched services but can't inform us whether these services are authorized to be there in the first place or not, it can detect misconfiguration of some firewall rules, but can't inform us about its correct complete rule set.

So what we really need is a holistic approach that can detect/validate vulnerabilities besides determine whether or not this very specific system comply with the entity's information security policy, in this case an IS audit needs to be added to our set of activities to perform a complete security assessment.

We won't be discussing vulnerability assessment and penetration testing within the rest of this article, and we will rather focus upon the IS audit process.

Let's start describing the IS Audit process from the very beginning, it is the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently [1].

It also provides management with a proper validation of the effectiveness of current controls of an IS.

Any information system can be modeled into four functional parts; Input, Processing, Output and Storage (IPO+S): Figure 1.

Any organization's management should manage to have efficient controls in place with regard to each part of this functional model.

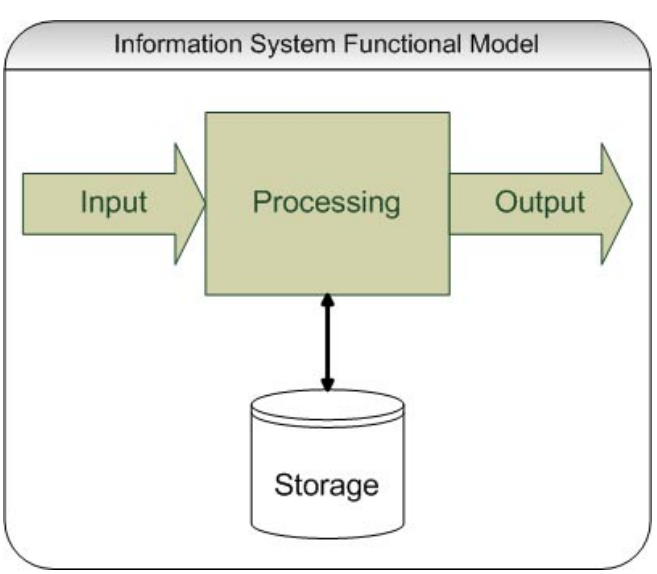

Figure 1. *Information System Functional Model*

Auditing Application Controls

When Auditing a certain application as a part of an IS, for example a core banking application, the auditor will audit the presence and effectiveness of the following controls:

Input Controls

- Edit checks are programmed into the application. They include:
- Error listing: Editing (validation) of data should produce a cumulative automated error listing. Each error should be identified described, and the date and time of detection should be given. Sometimes, the erroneous transactions may need to be recorded in a suspense file. This process is the basis for developing appropriate reports.
- Field checks: are tests of the characters in a field to verify that they are of an appropriate type for that field. For example, the field for a mobile phone number should not contain alphabetic characters.
- Financial totals: summarize dollar amounts in an information field in a group of records.
- A hash total: is a control total without a defined meaning, such as the total of the bank customers' account numbers, which is used to verify the completeness of data. Thus, the hash total for the bank's customers' accounts listing by the customer service department could be compared with the total generated during the end-of-day run.
- Limit and range checks: are based on known limits for given information. For example, hours worked per day cannot equal 25.

Lack of input controls might lead to injection attacks or fraud through manipulating

Processing Controls

- Programs used in processing should be tested, for example, by reprocessing actual data with a known result or by employing test data.
- Resources utilization on the processing computers should be monitored and compared to a base line.
- The auditor must make sure that the system always utilizes an audit trail so it can be used later if needed for example for accountability determination of certain event.
- End-of-file procedures should be available to avoid errors such as prematurely closing the transaction log when the end of the current master file is reached. The transaction log may contain new records to be added to the master file.

- Concurrency controls manage situations in which two or more programs attempt to use a file or database at the same time.

Lack of processing control might lead to running a malicious code that could for example deduct certain amount of money from each bank account and add all deducted amounts into a single account managed by the attacker, similar cases were identified more than once across the globe.

Output Controls

The auditor must make sure of the output controls as follows:

- The daily proof account activity listings (changes in database master files) should be sent to users for review.
- Error listings should be received directly from the system by a control group, which should make any necessary inquiries and send the errors to users for correction and resubmission.
- The console log should be reviewed for unusual interruptions, interventions, or other activity.
- Output should be distributed in accordance with distribution registers that list authorized users.
- End-of-job markers on the last page of printed output permit verification that the entire report has been received.
- Printer Spooler controls prevent access to spooled output, i.e. to a temporarily stored intermediate file rather than immediately printed, I once saw an unintentional bypass of this control within a certain system that used OS/400 on an AS/400 IBM machine where access controls were put on the payroll application, data and the spoolers that the HR team use for printing, but were not put on the rest of the spoolers, an HR employee were out of office at a remote branch and wanted to print some payroll report so it was sent to the unprotected spooler of a printer in that branch were it became accessible to everyone at that branch.
- Printed Reports should be properly handled as per its classification, for example a report containing customer names accompanied by their accounts' balances data should never be left in an unlocked place.

Sometimes the auditor relies through the audit process upon the user review of the output as a detective control, because users should be able to determine when output is incomplete or not reasonable, particularly when they prepared the input.

Lack of output control may lead to information disclosure of which in its turn may lead to impersonation attacks or used as part of a more

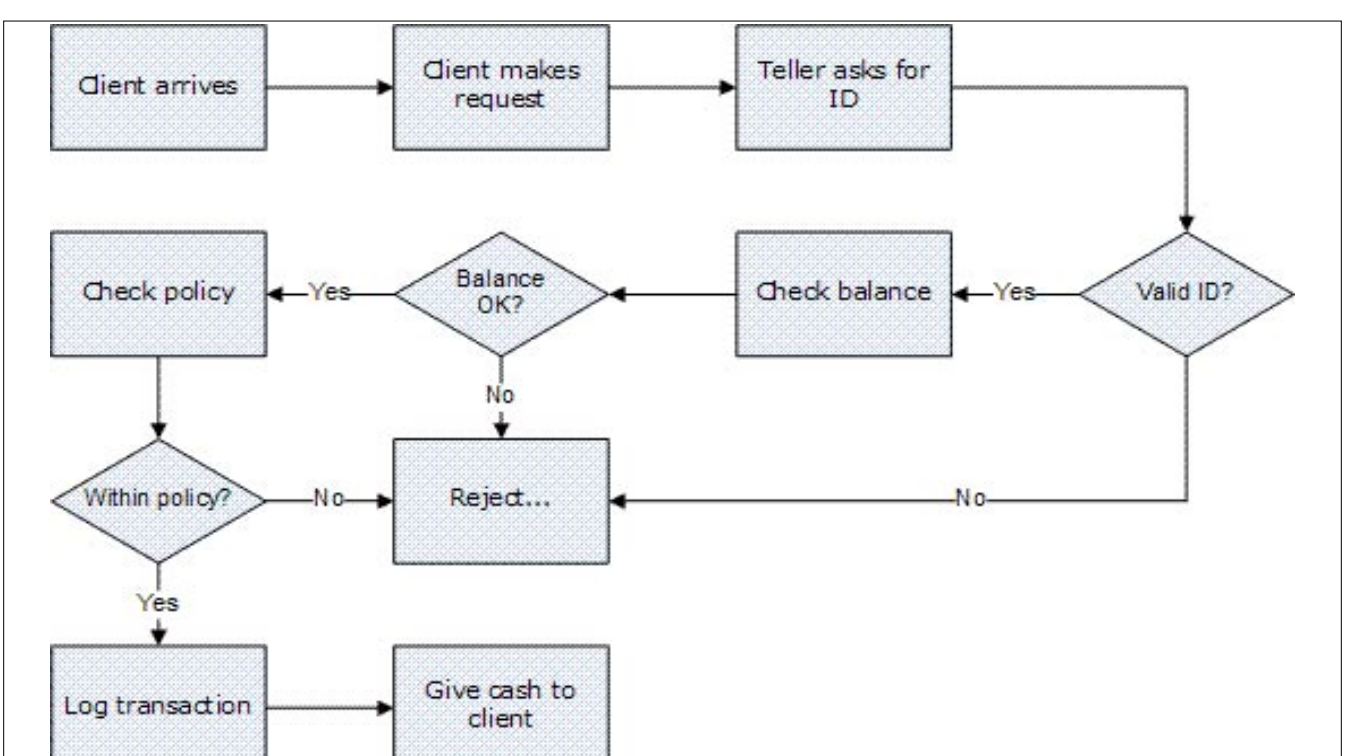

Figure 2. *Example of a flow chart of the bank teller [2]*

Table 1. *Customers Accounts Access Control Matrix*

User	Operating System	Accounts program	Accounting data	Audit Trial
Jasmine	rwx	rwx	r	r
Eric	rx	r	r	r
Scott	rx	r	rw	w
Charlie	rx	x	_	_

complicated attack like launching a phishing attack against the online banking customers after knowing their email addresses.

Storage controls

Some of the main storage controls to be audited are as follows:

Data Confidentiality

- Access controls
  - Restricting privileges either logically (through user credentials) or physically (through limiting physical access to data storage media only to authorized personnel even while on transit between one location and another).
  - Logical views (can be set though databases to make customized views of parts of certain tables to be viewed by users as per the need-to-know principle).
- Encryption
  - Encryption should be used while transferring data from one place to another, for example between a bank's branch and its Head Quarters (HQ) through network.
  - Any sensitive information e.g. customers' *Personal Identification Number* (PIN), should be stored in encrypted form.
- Media disposal
  - A media disposal policy should be in place to deal with disposing any media, whether degauss is used to erase data completely from magnetic disks or total physical destruction is used.

Data Integrity

Storage media hashing to prevent unauthorized tampering of data.

Data Availability

- Backup and recovery
  - Backup of database and logs of transactions
- High availability
  - Database replication, where the database is replicated to another server to maintain availability in case of main database loss or corruption.
  - Dual Logging, which involves the use of two transaction logs written simultaneously on two separate storage media so if one is lost or corrupted the other can still be used.

Lack of storage control can lead to information disclosure, unauthorized modification of data, inability to detect data manipulation in a timely fashion, inability to hold the person account for any found manipulation and can also lead to *Denial of Service* (DoS) attacks against the database without being able to bring it back online in a proper time.

There might be more industry/business specific controls that should be in place, so the auditor must be familiar with the industry of the entity to be audited, failure to detect a lack of the previous controls might indicate a fake secure status while, in fact, the IS under audit can be exploited via both insiders and outsiders (remember the media disposal policy) alike.

Table 2. *Excerpt of Audit Report Sample*

Control Objective	Control example	Test Performed	Conclusion
Security and confidentiality of application information is appropriate	User ID & Password are needed to access the application. Authorization matrix limits user access to authorized data only. Passwords are kept encrypted inside the database.	Reviewed related policies & tried to login to the application which requested user credentials Reviewed related policies, reviewed system configuration to assure compliance with policies Viewed DB table including passwords and found it clear text, administrator were informed and enabled the encryption on passwords store.	The control structure policies and procedures were suitably designed to achieve control objectives, however once control were not in place and it was mitigated during the audit

References

- Weber, Ron, EDP Auditing—Conceptual Foundations and Practice [1]
- Jew Mark, A Flow Chart of the Bank Samples, *http://businessoz.com* [2]

The IS auditor should also pay attention to general controls:

General Controls

- Access controls, including password length, age, history and complexity. It also includes firewall and *Intrusion Prevention System* (IPS) controls.
- System documentation, full documentation of the system design and source code (if it's home built) should be kept in a safe to provide aid later in case of code comparison and/or clean system build in case of system compromise. Also there should be a user manual to help with the user support.
- Data independence, where data storage should be designed independently from the application in order to facilitate integration with various applications and to facilitate auditing process.
- Segregation of duties, at least the function of operating the system should be segregated from the functions of database administration which should be segregated from the function of system analysis, design and coding/programming.
- Change management, where all software changes are appropriately reviewed and authorized.
- Disaster recovery plan, including regular creation of backup (duplicate) copies of data files, databases, programs, and documentation, Storage of backup files off-site, planning for auxiliary processing at another site.
- Background checks on applicants.

Tools/Techniques to be used in the IS Audit process

- Information Security (InfoSec) and *Information Technology* (IT) policies and procedures.
- A flowchart of the system under audit (Figure 2).
- An *Access Control Matrix* (ACM) that identifies the relations between subjects (users of the systems) and objects (various parts of the system) through allowed actions of each subject to each object Table 1.
- Knowledge of how to extract *Operating System* (OS) logs, *Database* (DB) logs and various logs and configuration details. Auditor may request certain reports from system administrators or run scripts that gather required data from the systems.
- Test data, which is specifically prepared sets of input data that test application controls by running a variety of transactions to be compared with previously determined results.
- Mapping, which involves monitoring the execution of an application to determine certain statistical information about the run such as *Central Processing Unit* (CPU) & Memory utilization of the system.

It is worth mentioning that the auditor should not audit the IS for the controls themselves but for the control objectives, for example access controls should provide reasonable assurance that only approved users have access to the system resources, and that they are accessing and processing only within approved boundaries. If the access controls are not efficient enough and fail to achieve these results then that must be stated clearly in the Audit Report.

Audit Report

There is no standard defined format for the audit report, yet it should include the control objectives, controls, tests performed and conclusion, such as the following sample excerpt for example: Table 2.

Conclusion

Through this article, we have discussed auditing the application controls and some of the general controls to be tested and clarified the consequences of failing to report lack of such controls showing that IS Auditing is an effective part of holistic security assessment, it identifies the existence and effectiveness of controls inside an organization and whether they achieve that organization control objective or not.

AHMAD TAHA ZAKI

Ahmad (@ahmadtaha) works as Network & Security Services Manager for Amiral Management Corporation, taught IS audit to CPA and CMA students at Ersnt & Young for many years. Ahmad has has more than 12 years of Information Security experience, a major in accounting, and currently completing his Masters degree in Computer Science. His industry certifications include:

- ***Certified Information Systems Security Professional (CISSP)***
- ***Offensive Security Certified professional (OSCP)***
- ***GIAC Certified Incident Handler (GCIH)***
- ***Microsoft Certified Systems Engineer (MCSE)***
- ***Microsoft Certified Systems Administrator (MCSA)***
- ***Microsoft Certified Database Administrator (MCDBA)***

http://amnena.blogspot.com