International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.5, May 2013 DOI:10.15693/ijaist/2013.v2i5.29-32

A User-Side Framework for Security Auditing and Monitoring

Vineet Kumar Chauhan[1], Dev Kant[2], Arunendra Kumar Singh[3], Saurabh Mishra[4]
Department of MS-CLIS,IIIT ALLAHABAD

***Abstract*- Today, the data and assets are critical for all type of organizations and institutions. Computer abuses are made the adverse effect in society in term of crimes. It causes the worst effect on the organization resulting in the down of market, business loss and confidentiality loss. The Information Security makes an organization system more capable by confidentiality, integrity and its availability and helps an organization in auditing and monitoring. For an organization, we can try to put security to some extent but much of security means no productivity. We use all security control components, which an Information system needs. That needs auditing and monitoring based on the policies and risk assessment defined. Our framework is designed to be used for small-scale business & institution/ organizations without dedicated and specialist staff and with low level cost and conduct their business without wasting much more time for auditing and monitoring. This audit and monitoring framework seeks to collect the most needed information-required and take a decision on security of data and assets. We can provide the security by scaling parameters and classification of assets from auditing and monitoring.**

I. INTRODUCTION

The Information Security assets data have more problems with system risks in the system; it is based on the concept of need to know by the experts of the systems. The frame work is based on the by this term that information is not disclosed to any person who does not have a legitimate and demonstrable business and its legal terms and need to receive and send the all information. That will protect organization information from unauthorized disclosure and access and its, use, modification, and deletion in context of audit.

Our framework is basically designed for user for small-scale business & institution/ organizations with low level cost audit and conduct their business without wasting much more time for auditing process. This audit framework seeks out to collect the most needed information-required and take a decision on security of data and assets. We can provide the security by scaling parameters and classification of assets from auditing.

The methodology of this framework is based upon the use for process, strength and accurate assessment on the systems of organization and time requirement.

II. RELATED WORK AND APPROACHES

The traditional auditing mechanism focuses on system audit trail. But it's not a proper solution for fulfilling the needed security for the organization as traditional approach is not sufficient to cover different applications and systems such as intrusion detection system. It may be a cause of any loss for the organization. Portability systems uses ptrace or proc for system call tracing. In case of web server monitoring one can use ptrace or proc but significant performance penalty can arises in this case. ptrace or proc may be suitable for only specific case and have considerable overheads. User-level monitoring requires flexible mechanism to reduce the overheads. The approach presented in this paper for auditing and monitoring is sufficiently flexible for various applications. By following this framework a person can perform auditing and monitoring without having knowledge of kernel programming.

III. SCOPE FOR THE AUDIT FRAMEWORK

Organizations have an array of digital assets, electronic equipment, publications, web resources and datasets and records. Scope of the Audit Framework to research assets, administrative assets, output, publications, existing records management systems, management issue associated with these other resources.

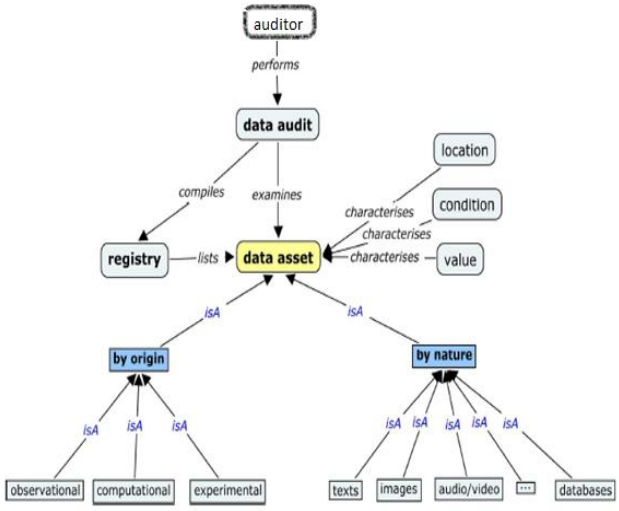

Fig. 1 Data Audit Framework scope

IV. THE AUDIT FRAMEWORK

To effectively fully realize, an organization must first be aware of three aspects of assets i.e place, circumstance and value. Conducting an audit will provide information that raising awareness of collection strengths and related issues to improve overall strategy. Data Creation and duration practice and services, suggesting policy change to lessen the risk faced.

A. Efficiency

Auditing provides sufficient information to indentify valuable data and assets. The information gained through auditing holding also assists in forward planning as it gives a more realize idea of infrastructure and storage requirements. Records of risks assessments also act as an audit for management decision, providing the level of resource dedicated to assets and data management and justification for the information security made.

B. Management at risks

The poor management and poor quality are widespread and potentially damaging the organization in terms of financial, legal and reputation. There are many scenarios in the departments which actions could put an organization at risk. The member /employee of staff which has been generated the problems or created or was responsible for the assets and data may leave before a new asset manager is assigned and duly checked.

Auditing improving the security functionality of management systems inevitably required an investment of time and resources. The benefits of auditing improved efficiency, risk management and reduction in risks, threat vulnerability, and the ability to fully exploit the value of data should outweigh these initial costs. This frame work provides more detail on preparing a business case and benefits to meet specific organizational needs.

C. How Audit Framework can help

The asset custodian/owner/user is orphaned to work can be identified and investigated further for specially meaning information gathering. This aspect do provide poor assets and data management practice, that means who is responsible for all data and assets, placing in the organization/institutional at risk if this person were to responsible for that. The classification process can believe the weakness in assets management. That allows you to take the organization in need a particular method for complete auditing means a storage and back-up costs is make to less if you do a regular audit in the has been set in the occurrence of disaster. Information is collected at this stage on assets and data and its management to highlight the weakness. To be provided to help ensure the audit organization can obtain significant efficiency savings, implement better audit management and improve reuse of resources.

The auditing process seeks to collect the required level of information required to take decisions how best to manage data assets in the long term.

1. How many department exits in your organization?
2. What is the statement of scope written in your certificate?
3. Do you have any well defined informal security policy?
4. How many different location your organization has presence?
5. How many different domains of security policy exits in your organization?
6. What is the size of IT infrastructure in your organization?
7. How many desktop your organization has? How many controls are applicable in your organization?

There are four stages that can be applied in this frame work method that is based on process and time calculating formula.

A. Plan to audit
B. Asset Classification
C. Risk Analysis
D. Reporting

This process manages and deploys the security risk in organization and does the audit in correct procedure and it will help for the low budget audit process.

A. Plan to audit

Audit plans have several “checkpoints”, and “matrix”. There are two key objectives of the planning stage: first to secure organizational buy-in by presenting a robust business case and second one to set up maximum probable in proceed of the audit.

Tasks for audit plan steps

- Auditor appointment.
- Approach all department of organization/ institutional.
- Conduct plan for the audit.
- Establishment and Set up the audit.
- Planning for all documents annually.
- Reports are on the time.
- Website and intranet.
- Research reports and publications.

B. Assets classification

This stage will result in assets and their managers, divided into groups according to their appraised value for the organization/institution. These all decisions will be approved by the management of the organization. The audits will form the main basis for stages of the audit where the assets and data are assessed and described in detail. The list prepared in, for stage plays a crucial role in the usefulness of later recommendations.

Before starting this stage, auditors should:

- Have understanding of departments of the organizations..
- Analyze organization’s assets and peripherals.
- Have a list of organization’s staffs and members and their responsibilities.
- Take a catalog of all IT systems and resources.
- Know about required implementation for securing the organization.
- Have a look of Workflow automation.

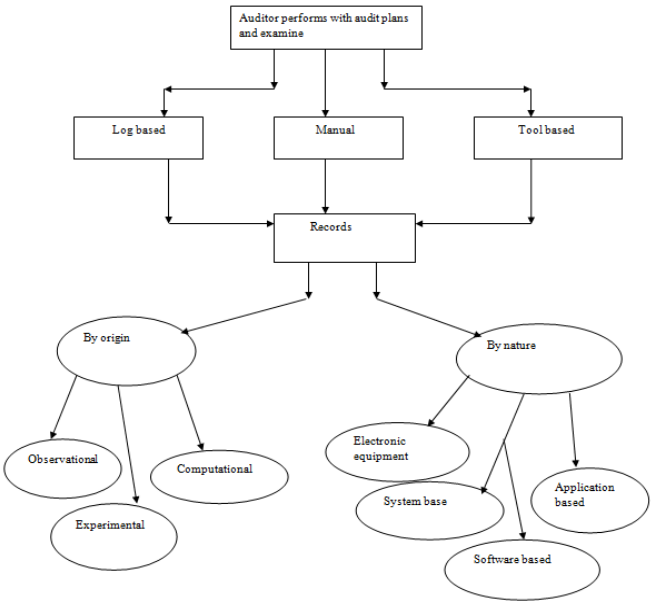

Fig. 2 Assets classification

The data assets identification should be proceed through the following steps:

- Analysis of resources;
- Conduct a survey;
- Preparing the data assets lists (including classifying identified assets|)
- Approving the asset classification and then finalizing it.

C. Risks analysis

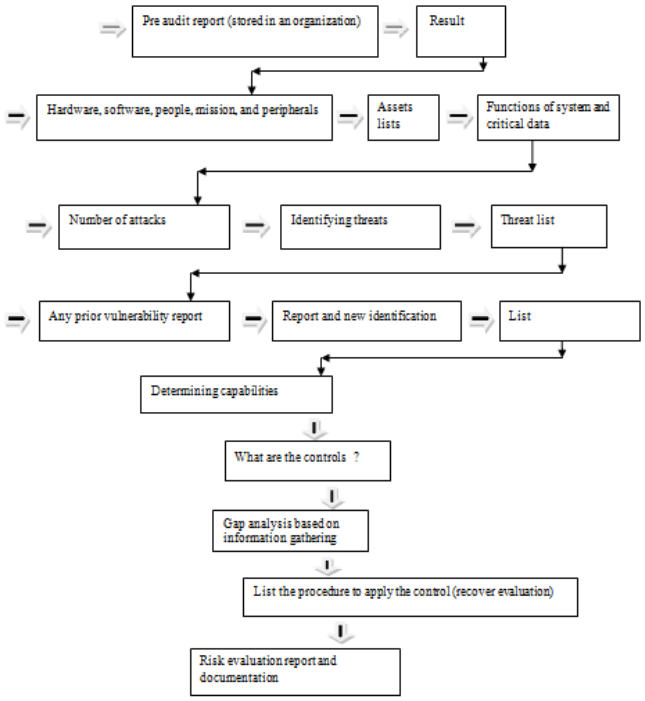

Fig. 3 Diagram for Risk Analysis

- ***Audit Risk***

Auditor should have to lessen the level of the risk to an acceptable level.

- ***Inherent risk***

An error could be considerable when it is combined with other errors during the audit shows there is no related controls exist.

- ***Control risk***

Error exists which are non prevented or undetected in nature on timely basis of the intended controls.

- ***Detection risk***

Detection risk can help in evaluation and access the auditor ability to test, identify and correct materials errors as the results of the test not exist when in fact they do, detection risk can help evaluate and access the auditor ability to test, identify and correct materials error as they result of a test.

D. Reporting

The audit report represents the outcome of the audit work. To write an effective audit report understanding of the way of using and viewing reports by the organization's departments is required.

Three main objectives of audit report are:

- Notification: By communicating the audit results, organization's departments would be aware about the situation.
- Convince: To encourage organization's departments that recommendations are valuable and valid.
- Outcomes: To provoke department's managers for taking proper actions.

V. MONITORING PROCESS

For internal control that is based on the controls provided in all different things for different organizations. In case of security reason the monitoring over the organization resulting in any miscommunication and different expectations cause problems within an enterprise. Problems are compound in term when, if not clearly defined not defined in law, regulation or rule for the organization. This will established with the needs and expectations of management and others. It describes in the term of control to:

- Design a model definition serving the needs of different parties.
- Provide a standard for business organizations for improvement.

VI. FORMULA

A. Evaluation of the effort (for time calculation)

This effort is actually for calculating the time based on the number of staff for auditing. Near about ¼ of the staff members are expected to be actively involved in auditing while is on the process with management and the remaining staff focusing on other activities. The number of staff will provide a nominal amount of time for the audit, most likely by completing another work. In the case of large departments

or institution it may not be feasible to speak to ¼ of all staff so the scope could be reduced.
So you can calculate a = d* h

Where,

a = estimated (supposed) time of auditors for auditing.
h = average number worked daily (5 hours).
d = number of days.

For k number of departments,

$$\sum_{i=1}^{k} a_i = d_i * h_i$$

If n = number of staff
nd = number of members who will involved in auditing for roughly 5 hours each (assumption because of business time)
ng = the remaining number of member involved in auditing for roughly calculated hours(t) each.

In practical, usually ¼ (supposed) of the staff members are involved in data management, either creating or curtain assets, and 3/4 (supposed) in other activities.
Then,

nd = ¼*n
ng = ¾*n
nd + ng = n

The estimation of the number of hours, h which the department staff will contribute to the audit based on standard departmental audit is,

$$h = nd*5 + ng*t$$

In the real world, cooperation and collections are different. In order to provide a more accurate estimation we should take into account a coefficient of complexity c which is based on the size of the department, the extent data holding and their compositing in terms of file formats, sizes and structure.

$$h = (nd*5 + ng *t)*c$$

For k number of departments,

$$\sum_{i=1}^{k} h_i = (nd_i *5 + ng_i * t_i)* c$$

Where,
c =coefficient of complexity (any emergency or sickness occurrence with worker)

B. Evaluation of the total effort

The total required effort for the audit v is the sum of the auditor's and department effort

$$T_0 = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} h_i$$

VII. CONCLUSION

We present a user side auditing framework suitable for auditing and monitoring for small scale business organizations/Institutions. We attain apparent auditing for the security of the auditing processes. We focus to prevent disclosure of sensitive information and unauthorized access in the organization.

The need for a security framework has never been more than now. Although various best practices and frameworks are being prevalently used, there is a growing and urgent need for a comprehensive framework that fulfills all the needs of an organization related to security. The proposed framework addresses this requirement. This framework is a generalized approach to information security and needs to be reviewed and revised by professionals and tested in the real environment. This study should be continued with a web-based survey to examine an IT professional's perception on security framework.

This audit and monitoring framework pursues to gather most required information and offers to take a decision on security of data and assets. With the help of this framework the security can be achieved by scaling parameters and classification of assets without wasting much more time for auditing and monitoring.

REFERENCES

[1]. Gregg, Michael, ISACA Books for Auditing For Auditor Exams
[2]. Cannon, David l. and Bergman, Timothy s. and Pampilin, Brady. CertfiedInformation System Auditor
[3]. Mayer, Nicolas and Heymans, Patrick, and Matulevicives, Raimundas,Information System Security Risk Management
[4]. Leiwo, Jussipekka and Zheng, Yuliang, A Framework For Management Of Information Security
[5]. http://www.symantec.com/connect/articles/ conducting-security-audit-introductory-overview
[6]. http://www.theiia.org/intAuditor/itaudit/archives/2006/april/preparing-for-the-security-audit-recommendations-for-beginner-it-auditors/
[7]. http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12356&section=text
[8]. http://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits
[9]. http://www.paramountassure.com/consulting/Information_security.html
[10]. http://www.data-audit.eu
[11]. http://www.oag-bvg.gc.ca/internet/English/parl_oag_199011_09_e_8004.html
[12]. http://www.isaca.org/Journal/Past-Issues/2002/Volume-1/Pages/The-IS- Audit-Process.aspx
[13]. http://www.paramountassure.com/consulting/information_security.html
[14]. http://www.kualitatem.com/security-audits
[15]. http://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview