Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Role of Log Management in Information Security Compliances

Akash Kumar Jain, Astitwa Bhargava, Ankur Rajput
RGNCLC, NLIU, Bhopal,
India

Abstract- Networks have millions and trillions of events per second and logs are recorded of each and every event hence management of logs is indispensable. Log management covers Log Collection, Centralized Aggregation, Retention and Rotation etc. Security incident and event management is used to find the security related events where as SIEM Enterprise solution helps in security, Compliance and troubleshooting. Message generated by SIEM Solution are known as Audit Records, Audit Trails and Event Logs. Mostly organizations faces a common problem i.e., to maintain records of logs in accordance to various Information Security Compliances separately. So to overcome this problem, the research paper has proposed a Log Management Framework (LMF) which covers all the requirements of major Information Security Compliances dealing with Logs. In the first section researchpaper had discussed the relationship between the event logs and Information Security Compliances like PCIDSSv3.1, ISO 27001:2013, SOX (2002), FISMA (2002),than the requirements of log management in accordance to the various Information Security Compliancesand at the end concluded with a combined framework for organization to follow LMF for complying with major Information Security Compliances.

Keywords- Log Management, SIEM, Information Security Compliance, PCIDSS, ISO 27001, SOX, FISMA

I. INTRODUCTION

Log management is a collective process consists of policies used for analyzing, evaluating, monitoring and disposing the large volume of data. Most of the times logsdatado not containsany useful information but some timelogs provides very useful information for security management. Logs have evolved to contain information related to many different events occurring within networks or in systems. Computer security logs are audit logs that track user authentication attempts and on the other hand security device logs are the logs thatrecord possible attacks. Log data contains a wide variety of information about the events and after analysis it becomeseasier to investigate and to set the accountability on any individual. Log data is to be preserve because it is an important source for digital forensics investigation too.

Log management is essential for security, accountability and for various information security compliances. Organizations store and analyze certain logs to comply with standard, legislation and regulations i.e.Health Insurance Portability and Accountability Act of 1996 (here and after refer as HIPAA),Gramm-Leach-Bliley Act (here and after refer GLBA), Federal Information Security Management Act(here and after refer as FISMA), ISO 27001:2013 and Payment card Industry Data Security Standard (here and after refer as PCIDSS) thathave several mandatory clauses related to log management. Many security solutions make information security compliance reporting easier as they directly provides the information security compliance specific report.

Example: Event Log analyzer analyzes events in organization A, and these changes are shown in log report in terms of log messages, hence the report made after analyzing any event can be shown in information security compliance audit, as PCIDSS 10.3 discuss about record trail events and 10.6.2 discusses for Review.

II. LOG MANAGEMENTANDEVENT LOGS

Log management is not a new concept; logs are generated from the day the computer evolves. Log management is the process for generating, transmitting, storing, analyzing the computer security log data. With the evolution of time the needs of log management is become diverse, i.e. in information security compliance, investigation, monitoring and many more. Information security Compliance as of become the forte of log management.

Event logs are the file that records sufficient events of the computer like the Login/Logout attempts of the user, changes in the file or error generated by any file, whenever these kinds of events occur the logs are generated and further used for investigation purpose and also for setting up the accountability. Events viewer is a tool that displays detailed information about events and it tracks the information in several types, i.e. Application Logs, System Logs, Security Logs, Setup Events and the Forwarded Events.

III. PROPOSED SYSTEM

Log managementdeals with large volumes of computer generated log messages. It is a better saying that each electronic Gazette leaves a trace and several information security compliances deals with log management Requirement in one or the other way. As say PCIDSS v3.1 Requirement 10 “Track and monitor all access to network resources and cardholder data” states about the logging of every events. ISO 27001:2013 Clause No. 9, 12 and 16 tells about Review, collection,

Retention and analysis of logs and several related events. SOX, FISMA, GLBA, HIPAA and many othersinformation security compliance covers the log Management requirement.

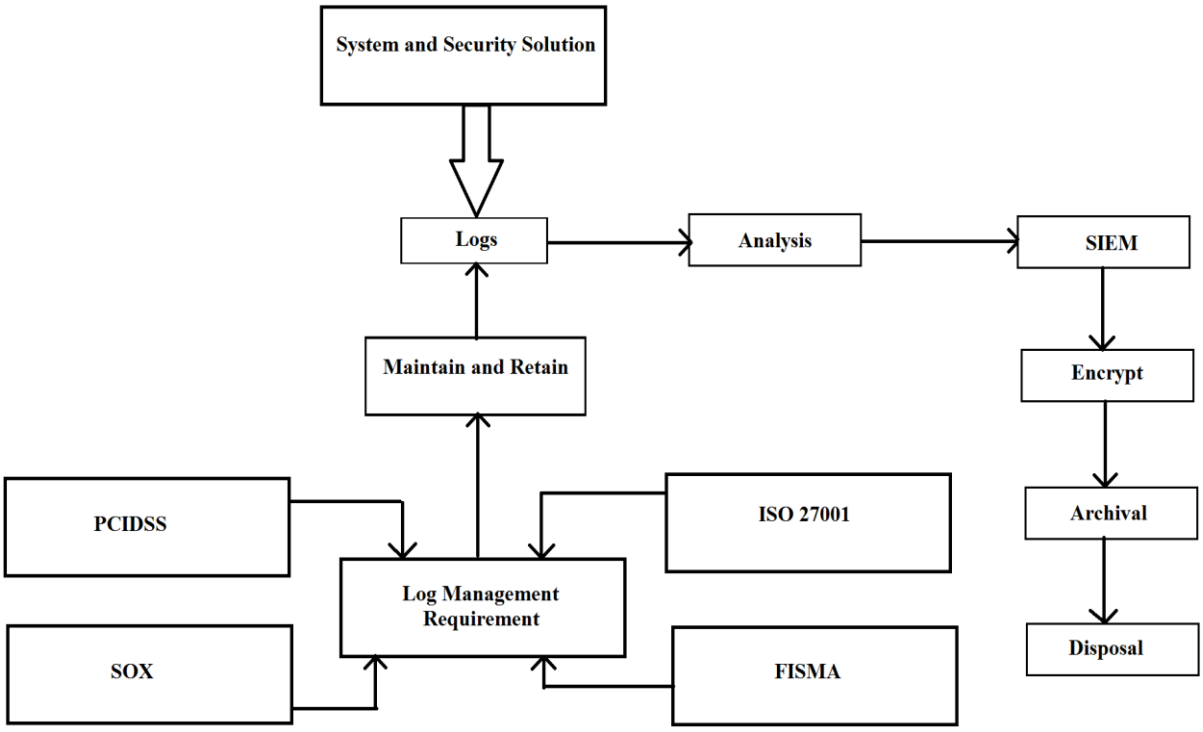

Figure: Log Management Framework in accordance with Information Security Compliances

The Figure gives the detail discussion of combining the information security Compliance requirement with Log generation byseveral system and Security Solutions. Here System and Security Solutions generate logs and that helps in identifying the security related events. Various information security Compliances with respect to several clauses do have log management requirements and these requirements talks about Collection, Retention, Analysis and Monitoring of various events for certain period of time with proper security, these system and security logs helps the organization for setting up the accountability and for fulfilling the information security compliance requirements. These logs are to be analyzed and security related events are to be carried out, for several purposes. After that all the logsbefore archivingare to be encrypted with proper encryption algorithm so that no unauthorized user can get access to the logs.All information security compliances mandate the Prevention and Retention of logs data for particular period of timebefore disposal.

IV. LOG MANAGEMENT FRAMEWORK

SIEM and Log Management play an important role to meet information security compliance requirement. Log management and SIEM can benefit an organization in several aspects firstly it helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time secondly reviewing and analyzing of logs for identifying events and setting the accountability. Now a day's logs are useful for forensic Investigation, auditing and there are number of information security compliances that directly or indirectly deal with the log management. Several organizations only maintains and retains the logs but if organizations covers other requirements related to logs then that can make their work easier at the time of information security Compliance audit. Information security Compliance do not mandate any special feature of log but it only specify to collect, maintain, retain, analyze, forward, continual check and audit the log files.

PCIDSS

Payment card Industry Data Security Standard is the standard made by several major payment brands. It is the widely accepted set of policies and procedures to optimize the security transactions and protect cardholder's data against misuse of their personal information. The Standard have 6 objective and 12 Requirements that deals with the storing, encrypting, maintain the card holder data and protecting it from unauthorized user. Recently RBI have mandate the use of PCIDSS for the organization which collects, retain the cardholder data. The Current version of PCIDSS is version 3.1 amended in 2015. The Below mention table discuss about the log management requirement in PCIDSS.

S.No.	PCIDSSClauses	Requirement
1.	10.1	Implement audit trails to link all access to system components to each individual user.
2.	10.2	Implement automated audit trails for all system components
3.	10.2.1	All individual user accesses to cardholder data

4.	10.2.2	All actions taken by any individual with root or administrative privileges
5.	10.2.3	Access to all audit trails
6.	10.2.4	Invalid logical access attempts
7.	10.2.5	Audit all the identification and authentication mechanisms changes, additions, or deletions to accounts with root or administrative privileges
8.	10.2.6	Initialization, stopping, or pausing of the audit logs
9.	10.2.7	Creation and deletion of system-level objects
10.	10.3	Record trail entries, User identification, Type of event, Date and time Success or failure indication
11.	10.5	Secure audit trails so they cannot be altered.
12.	10.5.1	Limit viewing of audit trails to those with a job-related need.
13.	10.5.2	Protect audit trail files from unauthorized modifications.
14.	10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
15.	10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
16.	10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts
17.	10.6.1	Record all security events, Logs of all system components that store, process, or transmit CHD and/or SAD, Logs of all critical system components Logs of all servers and system components.
18.	10.6.2	Review logs of all other system components periodically based on the organization's policies
19.	10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

ISO 27001:2013

ISO 27001:2013 "Information technology-Security techniques-Information security management systems-Requirements" is a Standard that clearly includes the organization, structure, policies, procedure, frameworks, guidelines, responsibilities and others. ISO 27001 is a standard fits to all organization either small or big and only deals with securing the Information and Information Assets. It helps organization to establish and maintain ISMS and used to maintain information security risk and to preserve CIA of an information and Information asset.

S.No.	**ISO 27001:2013Clause**	**Control**
1.	A.9.2.1	User registration and de-registration
2.	A.9.2.2	User access provisioning
3.	9.2.4	Management of secret authentication information of users
4.	A.9.2.5	Review of user access right
5.	A.9.4.2	Secure log on procedures
6.	A.12.4.1	Event logging
7.	A.12.4.2	Protection of log information
8.	A.12.4.3	Administrator and operator logs
9.	A.12.4.4	Clock synchronization
10.	A.16.1.1	Responsibilities and procedure
8.	A.16.1.2	Reporting information security events
9.	A.16.1.3	Reporting information security weaknesses
10.	A.16.1.4	Assessments of and decision on information security events.
11.	A.16.1.5	Response to information security incident
12.	A.16.1.6	Learning from information security incidents
13.	A.16.1.7	Collections of evidence

Sarbanes-Oxley Act, 2002

The Act drafted by Paul Sarbanes and Michael Oxley hence known as Sarbanes Oxley Act. SOX is a legislation passed by UScongress to protect shareholders and general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures. It was enacted after the series of high-profile financial scandals and was aimed at improving corporate governance and accountability. The act is not a set of business

practices and does not specify how a business should store records rather, it defines which records should be stored and for how much long time. SOX states that all business records, including electronic records and electronic messages, must be saved for "not less than five years." SOX Section302 and 404 somehow deals with Log management as it says each and every\thing should be recorded and monitored and proper reporting to be done.

S.No.	Clauses	Requirement
1.	Sec 302 (a)(4)(C) and (D)	Log in Log out Monitoring
2.	Sec 302 (a)(4)(C) and (D)	Logon Failure, Audit Log Access, Object Access, System Eventsuser accesses to the system berecorded and monitored for possible abuse
3	Sec 302 (a)(5)	Audit Policy Changes
4.	Sec 302 (a)(5)	User Access
5.	Sec 302 (a)(6)	User and Computer Account Changes
6.	Sec 302 (a)(6)	User Group Changes
7.	Section 404 (a)	Management Assessment of Internal Controls
8.	Section 404(b)	Internal control evaluation and reporting

Federal Information Security Management Act, 2002

FISMA is a management system that requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations, assets, including those provided by other source. FISMA get amended in 2012 and establishes a mechanism focuses on automated and continuous monitoring of cyber security threats and conducting regular threat assessments. The law itself do not prescribe any logging, log management it only prescribe the policy, planning and risk to federal systems. In accordance detailed guidance has been developed by NIST to cover the specifics of FISMA compliance.

S.No.	Clauses	Requirement
1.	AU-1	Audit and Accountability, Policy and Procedures
2.	AU-2	Auditable Events
3.	AU-3	Content Of audit records
4.	AU-4 & AU-11	Audit storage capacity, Audit record retention
5.	AU-5	Response to audit processing failures
6.	AU-6	Audit review, analysis, and reporting
7.	AU-7	"Audit reduction and report generation
8.	AU-8, AU-9 & AU-10	Time stamps Protection of audit information, Non-repudiation
9.	AU-12	Audit Generation
10.	AU-13	Monitoring for Information disclosure
11.	AU-14	Session audit

V. CONCLUSION

Log management plays asignificant role in an effective functioning of an organization.Logs can also be extremely useful in identifying security incidents, policy violations, fraudulent activity, and operational problems. They are also valuable when performing audits, forensic analysis, internal investigations, establishing baselines, and identifying operational trends and long-term problems. The Research Paper proposes a combined framework for an organization to comply with the major Information Security Compliances.So by implementing this framework, organization can achieve their various security and operational objectives.

REFERENCES

[1] Linda Volonino,Electronic Evidence and Computer Forensics, Communications of the Association for Information Systems, volume 12, Article 27
[2] Mayank Saxena, A review of computer forensics and logging system, ijarcsse, Volume 2, issue 1, January 2012.
[3] Bhanumathi.D, an Enhanced log record management system in cloud, Volume 5, Issue 4, 2015.
[4] Aamir Sohail, IT security using Arcsight ESM, ijarcsse, Volume 4, Issue 4, April 2014.
[5] Preeti Tuli, Priyanka Sahu, System Monitoring and Logging of Information and Crime Detection, ijarcsse, Issue 2, Volume 9, Sep 2012.
[6] Security Standard Council, PCIDSS Requirements and Security Assessment Procedures, Version 3.1, April 2015 https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.
[7] International Standard, ISO 27001:2013, Information Technology-Security Techniques-ISMS-Requirements https://trofisecurity.com/assets/img/iso27001-2013.pdf.
[8] Anton Chuvakin, Detailed FISMA Logging Guidance, April 14, 2011. http://www.infosecisland.com/blogview/12930-Detailed-FISMA-Logging-Guidance.html.
[9] IP Switch Inc., Network Management Division, Event Log Management for Security and Compliance Initiatives, July 2010.
[10] Olof Soderstrom, Esmiralda Moradian, Secure Audit Log Management, Science Direct.

[11] David Swift, Successful SIEM and Log Management Strategies for Audit and Compliance, SANS, Nov 4, 2010.
[12] Intel Security, White Paper, Log Management The foundation for Federal Security and Compliance.
[13] Dr. Anton Chuvakin, White Paper, the Complete Guide to Event and Log Management.
[14] Bernie Lantz, Rob Hall, Jason Couraud, and Locking down Log Files: Enhancing Network Security by Protecting Log Files, Issue in Information system Volume VII, No. 2. 2006.
[15] E. Casey, Error, uncertainty and loss in digital Evidence,IJDE, vol. 1, no. 2, 2002.
[16] Benjamin Boeck, David Huemer, A MinTjoa, Towards more Trustable Log Files for Digital Forensics by Means of 'Trusted Computing in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010
[17] Nobutaka Kawaguchi, Shintaro Ueda, Naohiro Obata, Reina Miya ji, A Secure Logging Scheme for Forensic Computing Proceedings of the 2004 IEEE Workshop on Information Assurance United States Military Academy , West Point, NY 10-Il June

