JISTEM - Journal of Information Systems and Technology Management
Revista de Gestão da Tecnologia e Sistemas de Informação
Vol. 11, No. 3, Sept/Dec., 2014 pp. *717-734*
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752014000300010

SECURITY INFORMATION IN PRODUCTION AND OPERATIONS: A STUDY ON AUDIT TRAILS IN DATABASE SYSTEMS

Rodrigo Roratto
Evandro Dotto Dias
Federal University of Santa Maria, RS/Brazil

ABSTRACT

Special care should be taken to verify the integrity and to ensure that sensitive data is adequately protected. One of the key activities for data loss prevention is anaudit. And in order to be able to audit a system, it is important to have reliable records of its activities. Systems that store critical data, whether financial or productive, must have features such as audit log, also called audit trail, which records all activities on critical data. This allows to identify harmful actions that can be internal or external, intentionally or unintentionally caused. Therefore, this paper presents major studies in security audit trail (audit log), especially records of logs, and it presents what is available in terms of commercial tools and what they offer.

Keywords: Audit trails, Information Security, Computer systems management technologies available, Computational Risk.

Manuscript first received/*Recebido em:* 28/11/2013 Manuscript accepted/*Aprovado em*: 26/06/2014

Address for correspondence / Endereço para correspondência

Rodrigo Roratto, Universidade Federal de Santa Maria, RS/Brasil. Email: roratto_rs@hotmail.com

Evandro Dotto Dias, Universidade Federal de Santa Maria, RS/Brasil, E-mail: evandrodotto@yahoo.com

Published by/ *Publicado por:* TECSI FEA USP – 2014 All rights reserved.

1. INTRODUCTION

Information is a critical resource in organizations. With the increased availability of computers for all -type users of around the world, more data is being processed in short periods of time. Understanding computer security requires understanding the meaning of threat, vulnerability and risk (Bosworth; Kabay, 2002). Vulnerability is a weakness in the computer system or its surroundings that may become a security risk.

A computer risk is the probability of an event resulting in a loss. Risks and losses may include financial and personal losses, loss of reputation and customer base, inability to function in a timely and effective manner, the inability to grow, and the violation of the laws and government regulations (Bosworth; Kabay, 2002). In systems where the device owner is not the person who owns the secrets in the device, an audit mechanism is essential to determine if there was any attempted fraud (Schneier; Kelsey, 1999).

Special care should be taken to verify the integrity and to ensure that sensitive data is adequately protected. Activities for data loss prevention is an audit. An audit process includes recommending actions to eliminate or minimize losses by identifying vulnerabilities and risks, to determine whether adequate security controls are in place, to ensure that security devices and audits are valid and to check controls; it also tracks auditing and security measures and whether they are working effectively (Bosworth; Kabay, 2002).

In many applications, access control and other information related to user operations should be kept in secure log files for intrusion detection and violations or for audit purposes (Xu et al. 2005). A lot of sensitive information is usually stored in log files. Therefore, it is important to ensure that if any system breach occurs, its logs are not compromised and the violation can be detected later (Xu et al. 2005). The first target of an experienced system attacker will be the audit trail/log system: the attacker wants to erase the traces of the attack, in order not to be detected, as well as keep in secret the method of attack so that the security flaws found are not detected by system managers (Bellare system; Yeey 1997). This shows that there is a great need to study and develop techniques to manage and especially ensure the inviolability of audit trails/logs, protecting them from damage and tampering with all types of users, whether intentionally or not. Based on these concepts, this research presents major studies in the pertinent area and tools available in the market.

Based on the aforementioned problems, we aim to present an analysis of key points that should be considered in the management of information security and a description of the main technologies and research relating to the application and protection of audit trails (logs). There is a lso a brief description of two of the major available commercial solutions on the market today. Thus, we seek to find solutions against violations, whether voluntary or involuntary, from any users or even the system administrators.

This paper is organized as follows: in section 2 the methodology used in this study is presented; in section 3, the concept of security information is presented. In section 4, the concepts of audit trails are shown; below in section 5, the use of logs in management systems databases are described; in section 6, major papers, researchseeking solutions for the protection of audit trails/logs are shown; in section 7, a brief description is available for managing critical data, offered commercially by the two leading providers of solutions, for information management and storage. Finally, section 8 presents the conclusions of this study.

2. METHODOLOGY

Regarding methodological procedures, this research is characterized as a descriptive and literature-based study, focused on a case study, as it describes models of audit systems and an analysis of attributes to be considered for the security of information systems of logs. It also seeks to identify what is most significant in research and solutions to the problem of audit trail security. The study is limited to theoretical analysis regarding solutions for the protection of audit trails (logs) and the tools available for managing critical market data. It is important to highlight that the term audit log is equivalent to audit trail.

3. SECURITY INFORMATION SYSTEMS MANAGEMENT

It is clear that businesses are increasingly dependent on technology and they need to provide confidentiality, integrity and availability. According to Albuquerque (2002) and Krause (1999) there are three basic principles to ensure information security, especially with regard to systems involving financial matters, such as:

•Confidentiality: the information can be accessed only by explicitly authorized personnel. It is the protection of information systems to prevent unauthorized access.
•Availability: the information should be available at the time it is needed.
• Integrity: the information must be retrieved in its original form (at the time it was stored). It is the protection of data or information from accidental or intentional unauthorized modification.

Some authors have suggested that where one person considers information to be safe, the system that manages it still must meet the following criteria:

• Authenticity: warrant that the information or its user is authentic.
• Non-repudiation: can not deny (in the sense of saying that something was not done) a transaction or service that modified or created information; can not deny sending or receiving information or data.• Legality: ensures the legality of (legal) information; adherence to a system of laws; and the characteristics of the information that has legal value within a communication process where all assets are in accordance with the agreed contractual terms or the existing national or international laws.

• Privacy: escapes from the aspect of confidentiality, because some information may be considered confidential, but not private. Private information may be viewed / read / changed only by its owner. It also ensures that information is not disclosed to others (in this case, the confidentiality nature of information is attributed). It is the ability of a user to perform actions on a system without being identified.

• Audit: traceability of the different stages of a business or process, identifying participants, locations and times of each stage. The audit adds credibility to the company and is responsible for the adequacy of the Company to legal and internal policies.

All these considerations about criteria for information security are added to another strategy for information management: accuracy. This means that the information must be grounded on true events or logical arguments, compatible with the needs of the organization. In this sense, it is not enough that the information is authentic, because its source can be dishonest. Reliability is not enough; accuracy of information must also exist.

4. AUDIT TRAILS (LOGS)

An audit seeks to identify and prevent suspicious and fraudulent activities by the user, collecting data about them in the database. The information collected is analyzed in order to find security problems and their origin (Simon et al. 2008). The main functionality of an audit is to provide secure and permanent storage of log records, so that they can be detected when a security breach has occurred (Xu et al. 2005).

The need to identify such activities and to determine suspicious patterns are important requirements for system security. In addition, an audit should be performed independently and transparently, so that all relevant information is classified (Hawthorn et al. 2006). An audit trail, which can also be called audit log, is used to ensure an accurate flow of transactions in a system. Every detail of a source and entry of a document or transaction should be made based on a report or file.

A digital audit enables the verification of the contents of a file system in a given period in the past. The audit protocol is a challenge / response between the auditor and the file system to be audited (Peterson et al, 2007).

The tracking technique can be applied in a single transaction for rapid testing; however, to ensure that control function consistently, the test should cover large volumes of data in different time periods (Bosworth; Kabay, 2002). Audit trails should be developed as a normal part of the internal control systems. Some systems can be acquired with the use of an automated audit log.

The system log file includes an entry for each operation applied to a database that may be necessary to recover an operation failure or an operating system failure; (Elmasri Navathe, 2004). We can expand the log entries so that it also includes the account number of the user and terminal online to be applied to each transaction recorded in the log. If any tampering with the database is suspicious, an audit of the database is performed, which is to analyze the log to examine all accesses and operations applied to the database during a certain period of time (Elmasri; Navathe, 2004). When an illegal or unauthorized operation is found, the DBA can determine the number of the account used to perform this operation. Database audits are particularly important for sensitive databases that are updated by many transactions and users, such as a banking database, which is updated by many bank tellers (Elmasri; Navathe, 2004).

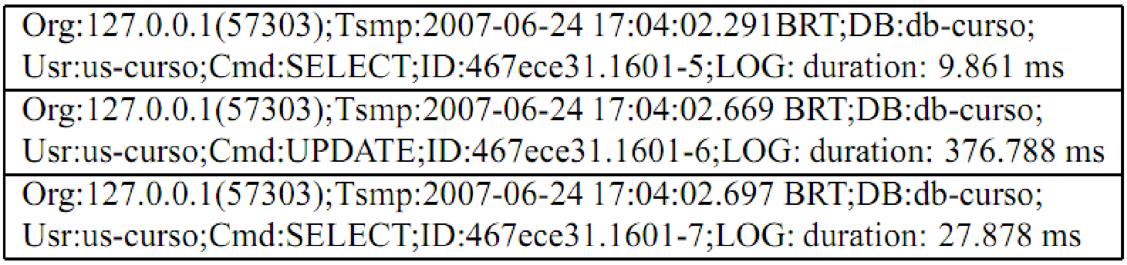
To prepare for a future audit, a file system generates authentication metadata that "commit" in the file regarding its current content system. This metadata is published in a third location. To conduct an audit, the auditor accesses the metadata and makes objections to the file system and crosschecks the information obtained from those represented in the metadata (Peterson et al. 2007).

The system must be prepared to withstand attacks with the creation of histories and fake versions that pass the audit process (Peterson et al. 2007). This class of attack includes creating fake versions of the data that matches the published metadata file, but differ from the data used in its creation. It also includes the creation of a fake history, the insertion or deletion of versions in a sequence without identity. This point describes the importance of an audit as an activity that aims to ensure the security and continuity business.

5. LOGS IN DBMSS

Saving logs on file systems is not recommended because if a file is deleted, there is no record of this action. This is a problem that occurs in a database (McDowall, 2007). Most DBMSs allow actions classified in the database, generating audit logs. Unfortunately, the methods generally are not transparent and many require the creation of triggers for each analyzed object (Simon et al. 2008). The use of triggers is not recommended as it burdens the use of the database by adding routines that must be performed to every action performed (Sallachl, 1992). The generation of audit data can be implemented via generic functions or through of database use policies and automated logs.

In order for log records to be created, there should be a separate record of all entries of audit trails associated with the creation, modifications and deletion of data and records in the database (McDowall, 2007). Regardless of the approach, each packet in the system must have a single audit trail. The advantage of this approach is that all audit entries are closely associated with the data they represent. This approach allows to search more specifically and quickly log records (McDowall, 2007). As an example of the generation of the DBMS logs, PostigreSQL will be presented. OPostgreSQL enables the system to manage records about its activities in its configuration file. Among the parameters present in this file is the creation of a log for each activity performed by the DBMS. This log can contain, in addition to information on access to data, several others, such as connection messages, authentication errors and errors of SQL queries. An example of log records generated by PostgreSQL is shown in Figure 1 In this case, the configuration file is defined to generate information on data accesses. As can be observed, the records are created in every query made by a client, in which the information about types of queries and their duration is present. These are the parameters that will be used as the basis for the audit.



```
Org:127.0.0.1(57303);Tsmp:2007-06-24 17:04:02.291BRT;DB:db-curso;
Usr:us-curso;Cmd:SELECT;ID:467ece31.1601-5;LOG: duration: 9.861 ms
Org:127.0.0.1(57303);Tsmp:2007-06-24 17:04:02.669 BRT;DB:db-curso;
Usr:us-curso;Cmd:UPDATE;ID:467ece31.1601-6;LOG: duration: 376.788 ms
Org:127.0.0.1(57303);Tsmp:2007-06-24 17:04:02.697 BRT;DB:db-curso;
Usr:us-curso;Cmd:SELECT;ID:467ece31.1601-7;LOG: duration: 27.878 ms
```

Figure 1: Example of log PostgreSQL (SIMON et al. 2008).

6. STUDIES FOR EXISTING SECURITY AUDIT TRAILS

In this section, we present published papers that directly or indirectly present contributions to the problem of violation of log records.

6.1 Forward Integrity for Secure Audit Logs

A log entry consists of a date (time) and event description. An experienced system attacker tries to modify or destroy log data corresponding to their current or past login attempts (Bellare; Yeey, 1997) .The authors of this paper, Mihir Bellar and Bennet S. Yeey, introduce a new security property which they called "forward integrity" (FI) based on the generation of message authentication codes (MACs) model. The goal is to prevent FI alteration or entering of information by the attacker, even when the log records become available to the attacker who gained control of the entire system.

In the MAC system, if an attacker obtains the MAC key, he/she can forge all the registry entries. In the FI system, the possession of the key at a particular point in time does not allow the attacker to forge log entries from a previous to the current date. Thus, the attacker can not change the contents of the log (Bellare; Yeey, 1997). He/she can even delete entries, but spaces will be visible in the registry and also the occasional transmission of the log to a remote system mitigates the effect of the deletion of records.

6.1.1. Message Authentication Codes (MACs)

Typically, MACs are used in a context of communication, where the sender and receiver share a secret MAC key. The sender uses the MAC key to generate a message and attaches it to the message; the receiver, who knows the MAC key, can restore Mac and accept as true only those messages for which the regenerated MAC matches the transmitted MAC. The MAC security model is the fact that it is computationally infeasible for an adversary-based network that does not know the key to modify the MAC messages and MACs for the receiver to accept them as true.

Once the audit logs are simply messages that are read and checked later on by a recipient and not (necessarily) over a network, it might simply attach MACs to the audit log entries to protect them. The following is a log coding scheme MAC.

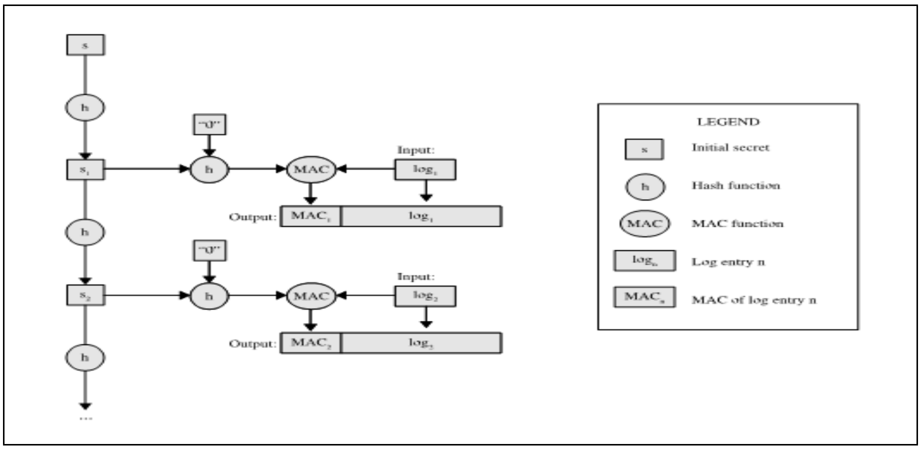


Figure 2: Example of MAC coding (HOLT, 2006).

However, the MAC model fails when it does not send continuous logs to a remote device, either by lack of or delay in transfers. Another vulnerability is in the fact that if an attacker enters the system and obtains the MAC key, they will get control of the logs (Bellare system; YEEY 1997).

6.1.2. Model forward integrity (FI)

This new model proposed by Mihir Bellar and Bennet S. Yeey makes use of MACs in a different way, avoiding the requirement of replication of a log in remote logs. A log entry consists of a date (time) and description of event. As previously mentioned, an experienced attacker attempts to compromise the previous data: they want to change or delete the entry corresponding to their attempts to login. In the same model proposed, even if the attacker gets the key in a given period in time, they will not be able to change records generated prior to this period (Bellare; Yeey 1997). They can even delete entries, but spaces will be visible in the registry and also the occasional transmission of the log to a remote source decreases the chances of complete destruction of records.

In this system, the keys are changeable and evolve in time periods, being generated from the previous key. The key Ki at time i is obtained with non-reversible function Ki-1 of the previous time and the current time. After the new key Ki is generated, the Ki-1 key is deleted. Thus, if an attack on attacker gets key Ki, they can not get Kj for j <i. This prevents the attacker from creating registry entries for previous

periods. A key K0 is provided for verifying the integrity of all independent versions of time. In this article, it is suggested audit log systems where:

$$log\_fn_j(m_i) = (m_i, FIMAC_j(m_i))$$

the generators of log messages (mi) may have or not control over when the registry decides to change the time. Each message received in one mi Ej time, the generator creates a log entry _fnj (mi) and saves the audit log which can be subsequently verified. The FIMACj (mi) is an authentication code attached to messages.

The cryptographic protection should be made very carefully. Do not just encrypt with a public key and make the verifications. If an attacker accesses the encryption key, they simply opt out the original record and generate their own logs. In addition to encrypting these secrets, the generator logs must authenticate its use at the beginning of the log, perhaps using a times tamping protocol (Bellare; Yeey 1997). This would require some communications network or digital signature scheme based on the key. Instead of generating codes in the data logger, the key may be generated by an external device. For example, the log is generated safely and delivered to the logger using an encrypted protocol with forward secrecy (FS). Maintain records in the filing is also essential not to allow an attacker to retrieve logs from a previous period, something that can only be avoided if a key system check (FS) is used.

6.2. Building an Encrypted and Searchable Audit Log

In this work the authors develop a study to create a search engine for keywords and encryption of log files. Delegation of resources is important so that a researcher can search and find specific entries in log files (Waters et al. 2004). They developed a system based on keys that allows you to search keywords on encrypted data using Identity-Based Encryption (IBE).

If at any time you want to search the auditor, an audit log to identify entries matching a certain keyword, they should go to the depositary audit agent. If the depositary considers it appropriate, they grant this ability to auditor. They can then search through the entries and see what entries correspond to the keyword. To audit entries that match the keyword log, the investigator can decrypt the input and display its contents, according to figure 4.

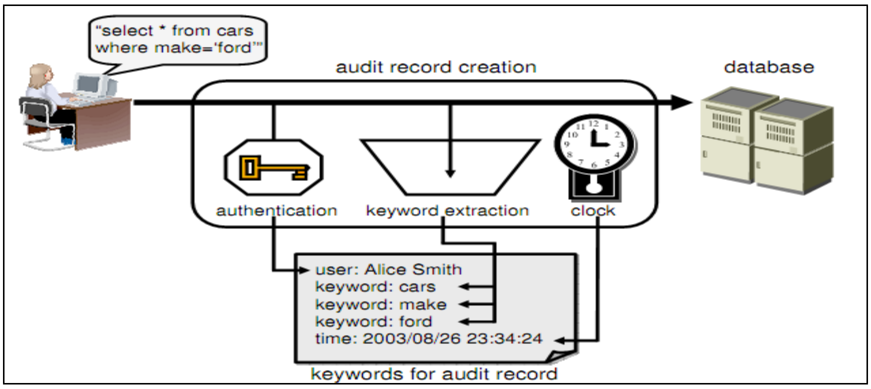


Figure 3: Scheme seeks records in an encrypted log (Waters et al. 2004).

6.2.1. System Operation

Operations in the asymmetric regime are significantly more expensive than the symmetric regime. The main obstacles are of modular exponentiation calculations for each matching keyword (Waters et al. 2004). However, if the same keywords are used frequently, the intermediate results can be reused. The asymmetric model corrects many of the drawbacks of the symmetric scheme (Waters et al. 2004). Since each server stores only public parameters, there are no secret keys for an attacker to steal .This model does not allow the attacker to search or decipher any entries in the audit that have already been generated and stored.

In that work, a system database audit that creates asymmetrically encrypted and searchable log entries was implemented. The log agent is implemented as a MySQL Proxy server, upon receiving a query, records the query, and passes it on to the server MySQL database.

The proxy is created on a Linux platform and is multi-threaded so that multiple users can be served simultaneously on the logging component that runs in parallel with the rest of the system. The audit log server assigns the date and time for each entry audit log. The log entries are written in another MySQL database server, which is dedicated to storing log entries. The software has a cache server that is used to reuse queries. It is implemented as a simple hash table that associates the result with the word sought. The method of checkpoint hash chain was also implemented. The audit log server calculates the present value of the hash chain for each log entry that builds. The current hash value can be read at any time. A part that reads this value can check the integrity of the log later on.

In this research the authors presented the implementation of a model that allows you to make searches through keywords in logging and ensure that these records will be protected via asymmetric key model.

7. SOLUTIONS FOR SECURITY LOGS IN DBMSs

Functionality and security is the biggest problem in any DBMS (Jangra et al. 2010). There are many problems?? in the DBMS market. Currently, we have several databases such as: Alpha Five, DataEase, Oracle database, IBM DB2, Adaptive Server Enterprise, FileMaker, Firebird, Ingres, Informix, Mark Logic, Microsoft Access, Microsoft SQL Server, Microsoft VisualFoxPro, MonetDB, MySQL, PostgreSQL, Progress, SQLite, Teradata, CSQL, OpenLink Virtuoso, Daffodil DB, etc. OpenOffice.org Base

Among these databases presented, which are more present on the market are: Oracle, IBM DB2 and (Jangra et al. 2010). The following are the features that each offers for the management of audit logs.

7.1 Oracle Database Vault

The Oracle Database Vault in 11g helps to protect sensitive application data and even the access of privileged users. Thus, customers can increase the protection of their sensitive application data from unauthorized access of any user, including the highly privileged ones, including DBAs and other powerful applications, to access sensitive data and applications on Oracle databases outside the scope of their responsibilities (ORACLE, 2010). For example, you can restrict administrative access to employee salaries, customer medical records, or other confidential information.

It can also be used to determine the separation of duties within the database; for example, blocking access to confidential DBA application data, but it allows it to perform the day-to-day activities such as backup and recovery, and tuning and replication of the database. It allows you to consolidate the databases of applications and to determine strong boundaries and policies around the access to data.

Regulations such as Sarbanes-Oxley (SOX), Healthcare Insurance Portability and Accountability Act (HIPAA), Basel II and Data Security Standards (DSS) of the Payment Card Industry (PCI) require that companies consider separation of duties and strong access controls to confidential information as shown i table 1 (ORACLE, 2010).

Table 1: Regulations and potential threats to security (ORACLE, 2010).

Regulation	**Potential security threat**
Sarbanes-Oxley Section 302 Section 302 of Sarbanes-Oxley	Unauthorized modification of data
Sarbanes-Oxley Section 404 Section 404 of Sarbanes-Oxley	The modification of data, unauthorized access
Sarbanes-Oxley Section 409 Section 409 of	A denial of service, unauthorized

Regulation	**Potential security threat**
Sarbanes-Oxley	access
Gramm-Leach-Bliley Gramm-Leach-Bliley	The unauthorized access, modification or disclosure
Health Insurance Portability and Accountability Act (HIPAA). HIPAA 164.312 HIPAA 164,312. Basel II – Internal Risk. Management Basiléia II CFR Part 11 CFR Part 11 Japan Privacy Law Japan. EU Directive on Privacy and Electronic. Communications Management of EU. Payment Card Industry Data Security Standard (PCI DSS) Payment Card Industry Data Security Standard (PCI DSS)	Unauthorized access to data

This system allows you to create flexible security policies for your database. For example, any user of the database, such as SYSTEM, who has the DBA role can make modifications to basic parameters of a database. Suppose that an inexperienced administrator, who has system privileges decides, to start a new log file, but they are not aware of the fact that if they do it at a particular time, this may cause problems to the database. With Oracle Database Vault, you can create a rule to prevent the user's command to make these changes, limiting their use of the ALTER SYSTEM SWITCH LOGFILE (ORACLE, 2010) .This tool also allows you to attach rules to the command rule to restrict further activities, such as limiting the execution of an instruction.

A database consolidation can result in multiple powerful user accounts residing in a single database. This means that besides the DBA database general, a proprietor scheme of individual applications may also have powerful privileges. Revoking some privileges may adversely affect existing applications. The Database Vault has a system called Realms, which allows to access applications through a trusted path, preventing database users, the database that, who have not been specifically authorized, from privileges and access to application data. For example, a DBA who has the SELECT ANY TABLE privilege can be prevented from using that privilege to read data from the application (ORACLE, 2010).

The Database Vault is against unauthorized access to application data, as well as changes to the database made by anyone, even by privileged access, such as DBA, intentionally or unintentionally that may in any way be harmful, taking into consideration various factors such as time, authentication, and other applications.

7.2 IBM InfoSphere Guardium

Systems DB2 database provide an audit mechanism to assist in the detection of unknown or unanticipated access to data. The DB2 audit facility generates, and allows maintaining an audit trail for a series of predefined events in the database.

For the protection of mission-critical systems, most organizations have formal control change policies of that determine how and when employees and service providers can make changes to production databases. However, it is difficult to detect violations, making policies difficult to enforce. As a solution, the IBM InfoSphere Guardium provides the tool that promises to send real-time security alerts whenever major system changes are made. Among the features are (IBM, 2010):

> - **Fraud Protection for SAP Systems:** From client data to ERP and personnel information, SAP systems often contain sensitive information that must be monitored for compliance and audit purposes. Now, businesses can detect fraud in real-time through the monitoring of all user activities at the application layer, including activities by administrators and outsourced personnel. The new release of InfoSphere Guardium provides more detailed information about SAP users, making it easier for businesses to detect fraudulent activities without making any changes to their databases or applications.
>
> **Protection of SharePoint files:** SharePoint repositories often contain sensitive information such as corporate financial results and valuable intellectual property such as product design data, but they do not have the necessary controls to prevent misuse by insiders. Now, for the first time, businesses have continuous real-time monitoring controls making it easier to detect unauthorized access to SharePoint repositories.
>
> **Support for the Mainframe:** An often overlooked, yet critical aspect of database security is real-time monitoring and auditing controls for database and system administrators**.** IBM now offers enhanced database activity monitoring capabilities for IBM DB2 databases running on System z, allowing businesses to protect critical information from unauthorized access by administrators. For example, if a database administrator at an insurance company tries to access a client's social security number, salary and medical history, the system will immediately generate an alert for security and compliance personnel. The new version of InfoSphere Guardium 8 leverages IBM-developed mainframe technology to capture all database transactions with minimal performance impact.
>
> **Improved Compliance and Audit processes:** A critical part of any audit is the ability to demonstrate that compliance and exception reports have been reviewed by oversight teams and appropriate actions taken. With the new software, businesses will have improved flexibility to define custom workflows and share specific audit information with relevant audiences in their organizations. Together

> with the software's pre-packaged report templates for common regulations such as SOX, HIPAA and PCI, this capability will help businesses save time and money by significantly reducing time required to gather and report on compliance data required by auditors.
>
> • Lock and advanced Quarantine: Companies can selectively block individual users not to access the system for a certain period of time in the event of suspicious activity or unauthorized, thus avoiding the loss of valuable data until the activity can be investigated. For example, if an administrator of a database in a hospital access sensitive data from a patient, access this employee will be locked automatically without any manual, costly and prone to error change of databases and applications is required.

The Info Sphere Guardium allows simplification of regulation and security organizations with a single set of centralized and automated controls for a wide range of applications and database of companies (IBM, 2010). In addition to its automated monitoring capabilities, the new software helps customers comply with the regulation easier to provide more precise control of the information, ensuring privacy and integrity of corporate data and simplifying audits.

8. CONCLUSIONS

This work shows the importance of ensuring security, inviolability and integrity of information contained in a computerized management system. There was a study and description of the main research in proposing mechanisms for the protection of audit logs. With this, it is concluded that with the increasing dependence of critical data storage systems, we must develop new solutions for the monitoring and protection of these data.

Currently, there are few studies in the area with some implementations, but none of them introduced a great solution to the problem of security logs. Two commercial systems from Oracle and IBM that promise to solve the problems such as unauthorized access to sensitive information and integrity of audit logs are also presented. Based on this research, one realizes that this is a very promising and important area of study and is recommended to conduct further research in the area of control and information security through the use of Business Intelligence technologies.

REFERENCES

Bellare, Mihir; YEEY, S., Bennet. Forward Secure Audit Integrity For Logs. Dept. of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 1997.

BOSWORTH, SEYMOUR; Kabay, ME COMPUTER SECURITY HANDBOOK Fourth Edition. John Wiley & Sons, Inc. 2002 Canada. ISBN 0-471-41258-9.Pg 28-846.

Elmasri, Ramez; B. Navathe Shamkant. FUNDAMENTALS OF DATABASE SYSTEMS 4th ed. Copyright © 2004 Pearson Education, Inc. ISBN 0-321-12226-7.Pg 735.

HAWTHORN, P., B., Clifton, C., Wagner, D., Bellovin, SM, Wright, RN, Rosenthal, A., Poore, RS, Coney, L. Gellman, R., and Hochheiser, H . (2006). Statewide databases of registered voters: a study of accuracy, privacy, usability, security, and reliability issues. Communications of the ACM, 49 (4): 26-28.

HOLT, E., Jason. Logcrypt: forward security and public verification for secure audit logs. Internet Security Research Lab, Brigham Young University. ACSW Frontiers '06 Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54.

IBM. IBM InfoSphere Guardium. Found at: http://www 01.ibm.com/software/data/guardium/-in date: 20/12/2010.

Jangra, A .; BISHLA, D .; BHATIA, Komal; PRIYANKA. Functionality and Security Analysis of ORACLE, IBM DB2, SQL & Server. Global Journal of Computer Science and Technology. Vol. Issue 7 View 10. 1.0 September 2010 page 8.

McDowall, RD Validation of Spectrometry Software - Audit Trails for Spectrometer Software. Spectroscopy 22 (4) April 2007 Pg 16 to 18. http://spectroscopyonline.findanalytichem.com/spectroscopy/data/articlestandard/spectrscopy/172007/421873/article.pdf.

Alfred J. Menezes; VAN OORSCHOT C. Paul; A. Vanstone Scott. HANDBOOK of APPLIED cryptography. Massachusetts Institute of Technology June 1996.Pg 560.

ORACLE. Presentation of Oracle Database Vault. Found in: http://download.oracle.com/docs/cd/B28359_01/server.111/b31222/dvintro.htm&prev=_t&rurl=translate.google.com.br&twu=1&usg=ALkJrhjnhkUAHhpz2vIjNKVO8sXgsNt0kw#CEGCIECD, on the date of 10/11/2010.

PETERSON, N. J. Zachary; Randal Burns; ATENIESE, Giuseppe; BONO Stephen. Design and Implementation of Veri able fi Audit Trails for a Versioning File System. Proceeding FAST '07 Proceedings of the 5th USENIX conference on File and Storage Technologies in 2007.

SALLACHL, DL (1992) .A deductive database audit trail.In Proceedings of the 1992.ACM / SIGAPP Symposium on Applied Computing (SAC'92), pages 314-319.

SCHNEIER, Bruce; KELSEY, John. "Secure audit logs to support computer forensics." ACM Transactions on Information and System Security, 2 (2), 1999, 159-176.

SIMON, Fernando; DOS SANTOS, L., Aldri; Carmen S. HARA. An Auditing System based on analysis of log records. Informatics Department Universidade Federal do Paraná (UFPR). Regional School Database (ERBD'2008), Florianopolis-SC, April 2008.

Brent R. Waters; BALFANZ, Dirk; DURFEE, Glenn; Smetters, DK Building an Encrypted and Searchable Audit Log CiteSeerX -. Scientific Literature Digital Library and Search Engine (United States). In 2004.

Xu, Wensheng; CHADWICK, David; OTENKO Sassa.A PKI Based Secure Audit Web In IASTED Communications, Network and Information and CNIS, Phoenix, USA, November 2005 Found in:. Http://www.oracle.com/global/br/corporate/press/2008_mar/ Oracle_Database_Vault.html

APPENDIX 1

Table 1. MCDA methods (Adapted from Guitouni and Martel (1998))

No	Method	Author(s)
	Linear weighting and elementary methods	
1	Weighted Sum	Churchman and Ackoff (1954)
2	Lexicographic method	Roy and Hugonnard (1982)
3	Conjunctive method	Hwang and Youn (1981)
4	Disjunctive method	Chen and Hwang (1992)
5	Maximin method	Hwang and Youn (1981)
	Single synthesizing criterion or utility theory	
6	TOPSIS	Hwang and Youn (1981)
7	MAVT	Keeney and Raifa (1976)
8	UTA	Jacquet-Lagreze and Siskos (1982)
9	SMART	Edwards (1971)
10	MAUT	Bunn (1984)
11	AHP and ANP	Saaty (1980), Saaty (2005)
12	DEA	Talluri et al. (1999)
13	COPRAS	Zavadskas et al. (2007); Chatterjee et al. (2011)
	Outranking methods	
14	ELECTRE	De Boer et al. (1998); Dulmin and Mininno (2003)
15	ELECTRE I	Roy (1968)
16	ELECTRE IS	Roy and Bouyssou (1993)
17	ELECTRE II	Roy and Bertier (1971)
18	ELECTRE III	Roy (1978)
19	ELECTRE IV	Roy and Hugonnard (1982)
20	ELECTRE TRI	Yu (1992); Mousseau et al. (2000)
21	PR OMETHEE	Dulmin and Mininno (2003)
22	PROMETHEE TRI	Figueira et al. (2004)
23	PROMETHEE/GAIA technique	Dulmin and Mininno (2003)
24	NAIADE	Munda (1995)
25	ELECCALC	Kiss et al. (1994)
26	UTADIS	Doumpos et al. (2001)
27	MELCHIOR	Leclerc (1984)
28	ORESTE	Roubens (1980)
29	REGIME	Hinloopen and Nijkamp (1982)
30	PROMSORT	Araz and Ozkarahan (2007)
31	EVAMIX	Voogd (1983)
32	QUALIFLEX	Paelinck (1978)
	Fuzzy methods	
33	Fuzzy relationship hierarchy	Lin and Chen (2004)
34	Fuzzy set approach	Sarkar and Mohapatra (2006)
35	Fuzzy suitability index (FSI)	Bevilacqua et al. (2006)
36	Fuzzy weighted sum	Baas and Kwakernaak (1977)
37	Fuzzy miximini	Bellman and Zadeh (1970)
38	AI methods	Ng and Skitmore (1995); Vokurka et al. (1996); Kwong et al. (2002); Choy et al. (2002); Choy et al. (2003); Choy et al. (2005)
39	CBR	Ng and Skitmore (1995); Choy et al. (2003)
	Mixed methods	
40	Martel and Zaras method	Martel and Zaras (1990); Martel and Zaras (1995)
41	Fuzzy conjunctive/ disjunctive method	Dubois, Prade and Testemale (1988)

APPENDIX 2

Operational requirements identified for the purpose of criteria-based evaluation are as follows:

1. The maximum tender for the evaluation is MVR1.500,000.00.
2. The minimum tender for the evaluation is MVR25.000.00.
3. Different cost bands are evaluated differently.
4. Public announcement should be made for every procurement costing more than MVR25.000.00.
5. There is a minimum of two criteria for evaluation.
6. There can be more criteria for evaluation based on the procurement.
7. Allocation of criteria and weights are based on the needs of the organisation.
8. A pre-bid meeting is compulsory and it needs to be announced.
9. Specification should be provided to potential bidders during the pre-bid meeting.
10. Marking criteria with weights are provided in advance in pre-bid meeting.
11. All required documents should be submitted with the bid and the requirements need to be informed to bidders.
12. If any bidder requires, calculations procedures are explained.
13. All bids are submitted on specific date and time. All the documents are checked verified during the submission process.
14. It requires minimum three BEC members to evaluate bids.
15. Basis for evaluation solely depends on the information provided in pre-bid meeting.
16. Suppliers' bids need to be verified for correct information.
17. Suppliers' previous jobs are evaluated based on available information.
18. Submitted support documents are primary source of information and they are assessed.
19. Assess the bid price compare to the expected work.
20. Suppliers' performances are evaluated based on the criteria provided and according to the weights and marks in allocated schemes provided in advance.
21. Marks are allocated based on the criteria and weights provided during pre-bid meeting in relation to performances of suppliers.
22. Technical expertise is used to get advice and explanations on procurement of technical good and services.
23. A through check is made if the proposed goods or services meet the specified standard.
24. Every criterion is assessed independently from one another.
25. All the criteria need to be evaluated.
26. No ranking can be made in evaluation; rather, marks are allocated in evaluation.
27. Pair wise comparison cannot be done.
28. In evaluation stage no changes to criteria, weights and requirements should be made.
29. Incomplete bids should be rejected.
30. Evaluation calculations are shown to bidders if requested.
31. BEC needs to approve of the winner. Evaluation analysis does not grant awarding the bid to the winner.
32. BEC need to state the reason for selection of the specific bid.
33. Bidders are informed the winner but not marks.

34. If any bidder wants more clarification, evaluation calculations are shown.
35. No discrimination in evaluation.
36. Evaluation method needs to be accurate.
37. Evaluation method should be using reasonable amount of resources and provide reasonable results.
38. Evaluation method should comply with procurement rules and regulations.
39. Evaluation method should provide no chance of manipulation from both sides.
40. Evaluation method needs to help minimise complaints.
41. Evaluation method needs to support utility concept.
42. Evaluation method should be clear and easily understandable.