Available online at www.sciencedirect.com

ScienceDirect

Procedia Economics and Finance 26 (2015) 991 – 999

Procedia Economics and Finance

www.elsevier.com/locate/procedia

4th World Conference on Business, Economics and Management, WCBEM

Technologies And Methods For Auditing Databases

Ioan RUS [a]

[a] *"Petru Maior" University, Tirgu Mures, Nicolae Iorga,no.1, Tirgu Mures, 540088, Romania*

Abstract

This paper aims at identifying and presenting tools and techniques to help perform IT database audit. The study summarizes the issues relating to the national and international IT audit regulations. It highlights the key differences between audit and other forms of economic audit (e.g. financial, internal or statutory). The paper presents the main components of IT audit, namely data center audit, computer network audit, operating system audit, Internet servers audit, database auditing, application auditing, external access flows IT audit (e.g. radio access, access from mobile devices). Practical aspects of the study describe database auditing as an important element of IT audit process. Current trends are presented for processing and storing data in relationship with data storage centers, cloud processing and inclusion of mobile devices as data access terminals. The author makes a presentation of database components that are relevant to database audit. Database audited components concern: file system database, data dictionary, database objects, database customer analysis, data protection and backup system, security and data protection from database. The last part of the paper is dedicated to preparing a new practical approach regarding the audit steps and technical means used in databes auditing. Finally, the author emphasizes the importance of database auditing, of data security and of the need to develop new technical auditing methods which are to be in consensus with the rapid development of Information Technology.

Peer-review under responsibility of Academic World Research and Education Center

Keywords: IT auditing; tools and technology; IT audit standards; embedded computing systems; data center; client/server arhitecture; practical ideas; cloud computing; information technologies.

1. Introduction

The economy of the twentieth century aimed mainly for material production and capital needed to achieve this

* Ioan RUS. Tel.:4-4343-432.
E-mail address: irus@clicknet.ro

Peer-review under responsibility of Academic World Research and Education Center
doi:10.1016/S2212-5671(15)00921-1

goal was money. Now, in the twenty-first century, it has become increasingly clear that the major purpose for most activities is the "intellectual production", i.e. services, research and development, production, marketing, competition, etc., all using information as the most precious asset.

Daily activity both for firms and individuals is increasingly dominated by electronic processing of information, either Internet, Intranet or information systems of organizations. The crucial components of any information system (Rus, 2007) are: hardware resource, software resource, human resource and data. This last component is to be found in practice under two aspects: in the sense of information – as logical conceptual structures, respectively in the sense of that data – as the actual level of information measurement. Specifically, considering the "person" as a source of information, his or her feature is the "age", which in the sense of information is an information while "45" represents its actual value.

The orientation of economic activities towards processes that rely mainly on information (i.e. financial transactions, stock exchange quotations, establishing and negotiating prices, auctions, etc.) simultaneously stimulated by the rapid mutations in information technology caused the necessity of development and penetration of information systems, virtually, at all organization levels and furthermore in all nowadays social and economic processes. Auditing these more sophisticated information systems has also become a necessity to control the operation and the effects they produce. Particular emphasis should be given to activities in the field of financial and banking transactions (Danescu, 2007; Spatacean, 2011).

The database audit must provide management with relevant elements regarding the operating and protection of data within the organization. In this paper, we will focus on "database auditing", as a distinctive component within the information audit, since data of an organization are becoming increasingly important and vulnerable.

2. Problem Formulation

Information audit relates only to the components of the information system. Because of this, information audit cannot be included within other types of audit. Information audit seeks specific objectives, has specific procedures and uses specific tools (Rus, 2012). Objectives, processes, procedures, components and international regulations regarding this process are defined by the US non-profit association ISACA (Information System Audit and Control Association). The American Standard which establishes IT governance rules is called COBIT (Control Objectives for Information and Related Technology). For the purpose of this framework, information has seven important characteristics (http://www.isaca.org/Education/ COBIT-Education/Pages/default.aspx):

- **availability** – the information must be available at any time during the decision process;
- **integrity** – the content and accuracy of the data must be in accordance with the rules and expectations of the organization;
- **compliance** – the logical structure of information and its concrete values must reflect the actual level of processes it characterizes;
- **reliability** – the information must relate to the specific decision-making process that is served;
- **efficiency** – the information must be provided with the lowest consumption of resources;
- **effectiveness** – the information must be relevant, accurate and timely provided for decision making;
- **confidentiality** – the information must be provided only to users whom they are intended to be delivered.

The IT auditor should also consider that provision of certified information is designed to enhance investor confidence in the integrity and reliability of financial reporting process, and therefore reduces conflicts of interest between shareholders and management, according to Spatacean (2011).

In Eropean Union, the specific standards, ie ISO 27000 prescribe three of these characteristics: availability, integrity and confidentiality. European standards allow analysis of other analytical characteristics defined by the auditor.

Technologies, phases and technical methods used on international scale in database auditing are known, regulated and certifie (Davis et al, 2011). Hereby, we can mention only four of the international certifications offered by ISACA (Information System Audit and Control Association), according to Rus and Danescu (2010), Certified Information Systems Auditor (CISA) – for IT auditors; Certified Information Security Manager (CISM) – for computer security managers; Certified in the Governance of Enterprise IT (CGEIT) – for experts in the IT system governance; Certified in Risk and Information Systems Control (CRISC) – for experts in IT system controlling and risks.

In the context of IT audit technologies we mention that the most important components of a information system subject to an audit, are the following:

- Operating Systems Audit;
- Internet servers (Web Servers) Audit;
- Database Audit;
- Data Center and Disaster Recovery Audit;
- Audit of Applications;
- Internal Network (LAN) Audit;
- External Network (WLAN) and Mobile Device Audit.

From a technical standpoint each component must be audited with specific technical means. The technical means are, on a general basis, specialized software components for IT audit. There are also situations in which the audited software components can be both Software and Hardware. An relevant example is the NAT (Network Address Translation) function for IP address mapping from a local network into the IPs of the Internet service provider. This function can be executed by a hardware component of the network equipments (by the routers) or from the Internet server, but it can also be a software component installed on the Internet server.

In this paper we addressed the issue of auditing databases, precisely because data is a very important capital for organizations. The most important structural elements of a database to be audited (Davis et al., 2011, p. 244) are as follows: *Table Stores rows of time in one or more columns*; *Stored procedures*; *Triggers*; *Relations beetwin database Entities*; *View statements*.

Appropriate technologies for database auditing follow the steps to be taken in the database audit process and show how each analysis must be done. A 21 step checklist, the technology and practical way of solving them is described by Chris Davis et al. (2011), an American professor at Harvard University and IT auditor for major companies in the US. This paper describes the content of each IT audit step and the method or practical approach. These processes are described in Table 1, as an explaining component, of the method that we designed for a dashboard used in database audit (TBA_BD).

From the perspective of implementing these steps, in practice, there are many concerns for the development of specialized software components as functions of databases or software products designed for database auditing. We enumerate some of the specific software products used in database auditing without any special selection or hierarchy option: Croos-Platform Audit (http://www.enforcive.com/database-audit-software) – for auditing information systems with multiple database engines; DB Audit and Security 360 v5.0.1.20 (http://www.softtreetech.com) – for auditing Oracle, SQL Server, DB2, Sybase and MySQL database servers; Azure SQL Database Auditing basics (http://azure.microsoft.com/en-us/documentation /articles/sql-database-auditing-get-started/) – for auditing functions, data access, database scheme and sub-scheme changes; Idera's SQL compliance manager and ApexSQL Tools' ApexSQL Audit – for auditing SQL server databases (http://sqlmag.com/sql-server/database-auditing-and-compliance-products), and so on.

The problem that we have identified is that the results provided by the audit reports of specific software products are not uniform, and often have different meanings or containt. As analysts of the information systmen behavior, we found that managers of organizations, to whom these audit reports are addressed, assess with great

difficulty thei audit findings. In most cases, they do not have a scale of values to identify the performance, the functionalities and dangers of their own information systems, as resulting from the audit reports. Audit reports have specific IT field elements, a highly technical feature that is designed more to IT professionals than to managers and IT auditors.

In this context, the major problem we have identified, refers to the need for designing a comparative and independent measurement tool of the database auditing results. We agreed that this is the main objective of this study.

3. Problem Solving

In designing the solution for developing a comparative and independent measuring tool for database auditing results, we set the following assumptions:

- the seven characteristics of information according to COBIT standard (listed above) are important elements for the final analysis of IT audit;
- the seven characteristics of information according to COBIT standard (listed above) have different degrees of importance in the final evaluation of the audit report.
- the processes subject to verification in the database auditing process (e.g. the 21 steps listed in paragraph 2 and used in practical database auditing) are actual measurements in various aspects of the database audit;
- the designed measurement method must be able to be generalized, easy to apply and very clear for the decision makers.

Based on these assumptions we considered employing the Balanced Score Table (TSP) ("Balanced Scorecard") (Kaplan and Norton (2014) as adequate for the purposes of research. We defined five levels of assessment grades from 1 to 5 for each evaluated process as follows: 1 - improperly; 2 - accordingly; 3 - medium; 4 - high; 5 - very high. Grades shall be based on the IT audit reports obtained automatically for each database audited process and in relation to the approach degree of information characteristics. We thus obtained the table in Table 1 which we named Scoreboard Database Audit (TBA_BD).

The Scoreboard Database Audit (TBA TBD) method which we designed, has the following structural elements (assuming the lines denoted by "i" and columns by "j")

- the lines reflect the audited processes, "n" (i = 1, 21);
- the column list the basic features of information "m" according to COBIT standard (j = 1,7);
- for each information characteristic is given importance weights (p_j);
- for each cell of the table grades are given from 1 to 5, taking into account each audited process in relation to each audited feature ($N_{i,j}$). These are determined by various established methods for ranking the criteria (Briggs et al. (2003);

Table 1 - Scoreboard Database Audit (TBA TBD)

		Characteristics of information							
		availability	integrity	compliance	reliability	efficiency	effectiveness	confidentiality	Final Score
	Percent %				P_j				
Processes Database Auditing (PBDA)[Davis et al. (2011)]	1. Verify that the database is running a database software version the vendor continues to support								x
	2. Ensure that all approved patches are installed per your database policy								x
	3. Determine whether a standard build baseline has adequate security settings								x
	4. Ensure that access to the operating system is properly restricted								x
	5. Ensure that permissions on the directory in which the database is installed, and the database files themselves, are properly restricted.								x
	6. Ensure that permissions on the registry keys								x

	used by the database are properly restricted			
	7. Review and evaluate procedures for creating user accounts	$\mathbf{N_{ij}}$		x
	8. Check for default usernames and passwords.			x
	9. Check for easily guessed passwords			x
	10. Check that password management capabilities are enabled			x
	11. Verify database permissions are granted or revoked appropriately for the required level of authorization			x
	12. Review database permissions granted to individuals instead of groups or roles.			x
	13. Ensure that database permission are not implicitiy grated incorrectly			x
	14. Review dynamic SQL executed in stored			x

	procedures	
	15. Row-level access to table data	x
	16. Verify PUBLIC permissions	x
	17. Network encryption is implemented	x
	18. Encryption of data at rest is implemented	x
	19. The appropriate use of database auditing and activity monitoring.	x
	20. Capacity of database environment to support existing and anticipated business requirements.	x
	21. Evaluate how performance is managed and monitored	x
	the database environment	
	Weighted Average **(MP)**	**PF** **BD**

where:

p_j – is the weight of importance of a certain feature (j). These are determined by various established methods for ranking criteria;

MP_j – is the weighted average of a certain feature (j) and is calculated using the following formula

$$MP_j = \sum_{i=1}^{n} (p_j * N_{ij})/100$$

PF_{BD} – the final score is calculated using the following formula:

$$PF_{BD} = \sum_{j=1}^{n} (Mp_j)$$

- on the bottom line of the table we calculated the weighted average for each information feature (M_{pj});
- summing up the weighted averages, we obtained the final score of IT audit report regarding the database auditing (PF_{BD});

Using grades on a scale of values from 1 to 5, in our opinion, provides the Scoreboard Database Audit (TBA TBD) method with a high degree of abstraction and generalization, while particular defining of weights for each information feature offers the specificity required for different socio-economic fields. We refer to the fact that information "integrity" is not as important in a information system specific for rendering service industry compared with, for instance, financial transaction industry.

The number of audited processes and the referenced features are elements defined by the auditor, which provides flexibility and specificity to the the Scoreboard Database Audit (TBA TBD) method.

4. Conclusions

IT audit represents a specific information system audit. This paper highlighted the theoretical and practical aspects of this type of audit, by detailing aspects related of database auditing. We identified a problem in the interpretation and use of IT audit reports, by users who are not computer experts.

Followingly, we projected a new method for synthesizing IT audit reports which we entitled Scoreboard Database Audit (TBA_BD).

The Scoreboard Database Audit (TBA TBD) method offers clarity, simplicity, generality, specificity and flexibility in the presentation and interpretation of IT audit results.

It is also important that, in our opinion, this method provides a high degree of independence and comparability in the analysis of IT audit indicators.

References

Briggs S., Petersone B., Smits K., - Manual de metode folosite in planificarea politicilor publice si evaluarea impactului, Studiu Elaborat in cadrul proiectului Consolidarea capacității instituționale a Guvernului Romaniei de a gestiona si coordona politicile publice si procesul decizional", RO2003/IB /OT-10), © Secretariatul General al Guvernului Romaniei.

Comes C. A, Marian L.O., Ghisoiu N., Bircea I., - Business process management with Unified Modeling Language, WSEAS Transactions on Computers, Ag. Ioannou Theologou 17-23, Athens, 15773, Zographou, Greece, 6 (2), 2007, pp.361-366.

Davis C, Schiller M., and Wheeler K. – IT AUDITING, using controls to protect information assets, Ed. The McGraw-Hill companies, Osborne, New York, 2011, ediția a 2-a, USA.

Danescu T. - Audit financiar : convergente intre teorie si practica, Ed. IRECSON, București, 2007.

Kaplan R. and Norton D., – Using the balanced scorecard as a strategic management system, Harvard Business Review, [www.hbrreprints.org].

Rus I. - Audit Information Content- published in journal Annales Universitas Apulensis serie OECONOMICA, nr.14/2012, volumul 1, pag.119-127, Alba IULIA, 2012.

Rus I. - Informatica de Gestiune – Editura DACIA, colecția UNIVERSITARIA, seria INFORMATICA, Cluj-Napoca, 2007, 164 pagini, ISBN: 978-973-35-2310-9.

Rus I. - Model for Designing an Information System with High Reliability, published in journal STUDIA UNIVERSITATIS PETRU MAIOR SERIES OECONOMICA, 2014, vol. 1, pages 28-44, Tirgu Mures, 2014.

Rus I., Tatiana Danescu -The Information Audit – between necessity and regulation. published in volume APPLIED ECONOMICS, BUSINESS & DEVELOPMENT, Kantaoui, Sousse, TUNISIA, 2010, (AEBD' 10), ISSN: 1790-5109, ISBN: 978-960-474-184-7. http://www.wseas.org, pag.98-103.

Spatacean O., The Impact of Financial Reporting upon Stock Prices Evolution – an aproach based on financial contagion, Studia Universitatis Petru Maior Series Oeconomica Journal, Fasciculus 1, 2011, ISSN 1843-1127, ISSN online 2286-3249, pp. 87-104.

http://azure.microsoft.com/en-us/documentation/articles/sql-database-auditing-get-started/.

http://sqlmag.com/sql-server/database-auditing-and-compliance-products.

http://www.enforcive.com/database-audit-software.

http://www.isaca.org/CERTIFICATION/Pages/default.aspx.

http://www.isaca.org/Education/COBIT-Education/Pages/default.aspx.

http://www.softtreetech.com/.