American Journal of Science, Engineering and Technology
2022; 7(2): 39-43
http://www.sciencepublishinggroup.com/j/ajset
doi: 10.11648/j.ajset.20220702.12
ISSN: 2578-8345 (Print); ISSN: 2578-8353 (Online)

Study on the Audit of IT Security in Health Structures: Case of Health Structures in Burkina Faso

Yanogo Kiswendsida Jean Hermann, Kabore Baowendnere Tanguy

Institute of Computer Engineering and Telecommunication, Polytechnic School of Ouagadougou, Ouagadougou, Burkina Faso

Email address:

yanogohermann@yahoo.fr (Y. K. J. Hermann)

To cite this article:

Yanogo Kiswendsida Jean Hermann, Kabore Baowendnere Tanguy. Study on the Audit of IT Security in Health Structures: Case of Health Structures in Burkina Faso. *American Journal of Science, Engineering and Technology*. Vol. 7, No. 2, 2022, pp. 39-43.
doi: 10.11648/j.ajset.20220702.12

Received: March 22, 2022; **Accepted**: April 23, 2022; **Published**: May 12, 2022

Abstract: In this study, we want to show that despite the important and crucial data that health structures (hospitals, clinics, health centers etc.) manage, they do not take into account the risks of patient data leaks. As a result, these structures do not seem to favor computer audits on a regular basis in order to determine possible intrusion doors. some people think that data leaks are due to external factors which can be characterized by cyber-attacks coming from outside. Health care workers can take confidential patient information and expose it and without a security audit it would be difficult to find the fault and the person responsible, hence the interest of security audits. The research was done because we noticed that the health structures in Burkina Faso manage big and crucial data and they need to pay attention with. Data leakage situations can be crucial on the one hand for patients who will see their personal information end up in the public square and on the other hand discredit the image of the health structure and which will result in the non-attendance of this structure. In this study, the expected result is to show the existence of the negligence of health structures in Burkina Faso when managing patient data that can lead to a leak of this data, also to propose palliative solutions to the risks to which they are exposed. We went to meet the managers in charge of managing these structures in order to collect useful information and analyze it.

Keywords: IT Security Audit, Burkina-Faso Health Structure, Computer Security Risks, Leak of Data, System Management

1. Introduction

The IT audit can be defined as the set of techniques used to assess the level of security of a structure. They are essential for the survival of all structures. Health structures in Burkina Faso are highly exposed to security risks if the standards and rules governing the audit of IT security are not well respected. We seem to notice that the health structures neglect the permanent application of the IT security audit. The adoption the IT security audit should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization [1].

A security audit should meet the International Standard that has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) [1].

In Burkina-Faso, health structures are made up of public hospitals, clinics, CMAs, CSPSs, etc.

Continuously conducting IT security audit tests could prove to be the key to success in terms of protection for any structure managing important and sensitive data. The various alerts on the security risks faced by many structures challenge more than one to become aware of the measure. Are the health structures in tune with the standards, rules and periodicity for the implementation of security audits? Auditing of information security constitutes a key part of security operations taken inside organizations. Information security problems must be addressed as quickly as possible [2]. Several institutions believe that they are secure and are safe from all incidents

that their data or equipment could not suffer probable attacks. These institutions do not seem to add value to the IT security audit. Public hospitals, clinics manage important and confidential patient data that should not end up in the hands of a foreign person. It is therefore essential to take all the necessary and adequate measures to protect them.

In a world characterized by the digitization of activities, all structures are equipped with an information system that is more or less dematerialized. Medium, small and even large are all subject to the rule of having an information system. A malfunction in the existence of a gateway to your system can lead to data theft, an impact on the reputation of your structure, and even spying on your structure. The computer security audit makes it possible to make a statement of the vulnerabilities of your information system in order to compensate for all eventualities of intrusion. The IT audit is a process that is intended to be periodic in order to detect any risks that may affect the information system. The health structures in Burkina Faso, despite the security issues they face, seem not to respect the periodicity and the principles of the IT security audit, all of which expose them to enormous and permanent security risks. Structures that manage a large flow of data, such as hospitals, must permanently apply an IT security audit.

2. Materials and Methods

2.1. Materials

We used the quantitative method to collect our primary data. This method allows us to quantify by giving the real proportions of our results. In each health structure we exchanged with the person in charge of the computer system in order to collect information on the way in which they work. A structured questionnaire was prepared and an interview session was initiated. A validity, consistency, and distribution test was applied as a data verification technique. We used spss software to analyze our collected data.

2.2. Methods of Sampling

We used the following formula to determine our sample.

$$N= Z^2_{\&} *P*Q/ e^2$$

& = 0.5 implies that Z = 1.96;
P = 0.5;
Q=1-p=0.5;
E = between 1 and 10%;
N: represents the sample size;
Z^2 = reduced center normal law;
& = represents the degree of confidence;
e^2 = represents the maximum or systematic error.
We will therefore have

$$N= 1.962* 0.5*0.5/ 0.12= 0.2401/0.01 = 97$$

3. Presentation and Impact of the IT Security Audit

The life of health structures is marked by the manipulation and management of crucial data. When a patient's data arrives in the hands of a person who is not supposed to have it, it could cause inconvenience, hence the interest in doing so permanently. Indeed, the importance of information technology (IT) auditing has grown with increased reliance on IT for business operations and new regulations regarding the assurance of IT for these operations [3]. The IT security audit guarantees the availability of the information system, the integrity of its data, the confidentiality of access and provides reassuring evidence that makes it possible to know who is accessing, when, to such and such data or application. The IT security audit makes it possible to avoid internal and external risks. It can be done in-house if the skills exist there or call on seasoned experts.

4. Results and Discussion

4.1. State of Periodic Implementation of the It Security Audit

To the question of whether the health structures periodically carried out IT security audits, we obtained the following results:

Table 1. *Do you periodically perform IT security audits?*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	OUI	5	5,2	5,2	5,2
	NON	92	94,8	94,8	100,0
	Total	97	100,0	100,0	

This table is obtained on the basis of the data collected and inserted into the SPSS software.

It shows the proportions in terms of frequency, percent, and valid percent. It also shows that the total number of respondents is 97 and that the total sample was taken into account for the analysis. This table clearly indicates that structures that do not perform IT audits go up to 94.8% compared to 5.2%. If we export the data from the table to have a clearer view in terms of histograms we obtain the following figure:

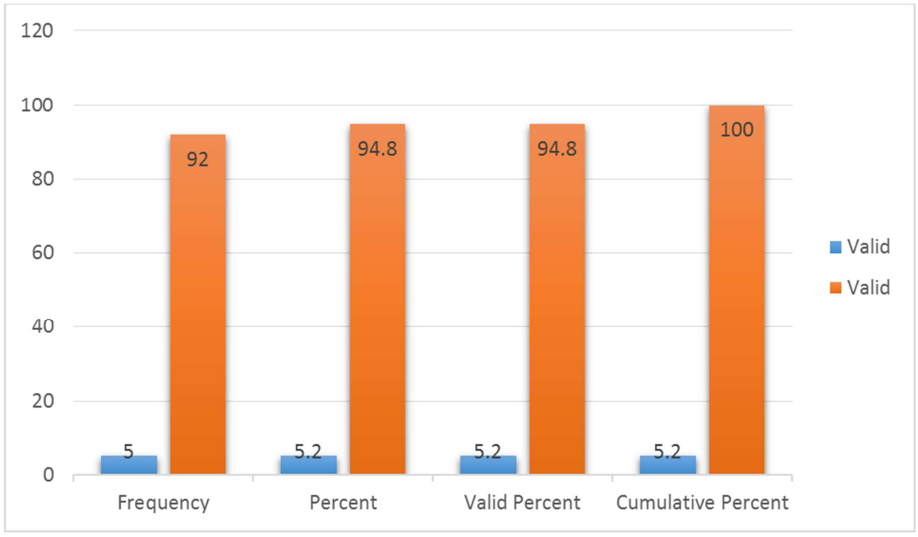

Figure 1. *Statistic comparative.*

Figure 1 shows that despite the importance of the IT security audit, we see the peak of 94.8% of those who do not apply the audit and this is not without consequence. Indeed, Security plays a major role in the healthcare domain. Preventing cyberattacks on healthcare infrastructures is no longer negligible. Compromising security in any Health system can lead to serious damage to patients' health [4].

4.2. State of Implementation of the Audit Based on the Problem That Has Arisen

To the question of whether the structures carried out audits only when there is a problem that arises, we obtain the following results:

Table 2. *Do you audit only when there is a problem that arises?*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	OUI	92	94,8	94,8	94,8
	NON	5	5,2	5,2	100,0
	Total	97	100,0	100,0	

This table was also obtained on the basis of the collected data and enters the SPSS software. This table gives the proportions in terms of frequency and percent. As we can see, 94.8% of structures are waiting for problems to arise before starting to investigate with the security audit. This way of working is not advisable and is not without consequences for these health structures. Only 5% of health facilities do not wait for a problem to arise before engaging in auditing as can be seen in Figure 2.

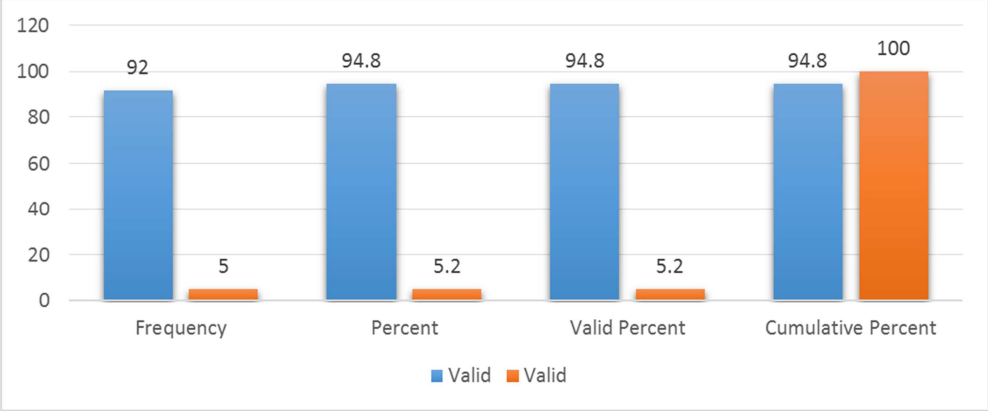

Figure 2. *Statistic on the mode of choice of the security audit.*

In Figure 2, we actually notice that the trend is up and this should not be the case. Indeed, in the standards, a security audit is a preventive approach. In fact, you should not wait for an incident to occur to set it up. The key to an efficient information system protected from all threats is anticipation. It should also be used at regular intervals in order to cope with the evolution of attacks because the Health sector's increasing dependence on digital

information and communication infrastructures renders it vulnerable to privacy and cybersecurity threats, especially as the theft of health data has become lucrative for cyber criminals [5].

4.3. State on the Consultation of the Logs

When asked whether the health structures consulted the logs, the following results were obtained:

Table 3. *Do you consult the logs in order to trace the unhealthy activities that have taken place?*

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	OUI	5	5,2	5,2	5,2
	NON	92	94,8	94,8	100,0
	Total	97	100,0	100,0	

This table is obtained by entering the data collected from the 97 people surveyed into the SPSS software. This table clearly shows us that 94.8% of health structures do not consult logs. We know, however, that the activities carried out within these structures could involve management and integrity risks, despite this no attention is paid to this regard. The permanent verification of the logs could participate in the reduction of the risks that their daily activities could cause. Only 5.2% of structures take part in a permanent review of their log.

Figure 3 essentially shows us a complete view of the statistics of consultations carried out by health structures in Burkina Faso. The percentages of 94.8 compared to 5.2 are alarming and are not without consequences for health structures in Burkina Faso. Indeed, we can say that a log, event or journal is the notification of an event of greater or lesser importance sent by a service, a system, a network element or an application. Information stored in logs of a computer system is of crucial importance to gather forensic evidence of investigated actions or attacks and analysis of this information should be rigorous and credible [6]. The logs have an interest and a crucial importance in computing, because it is a question of knowing what happened on a set of applications.

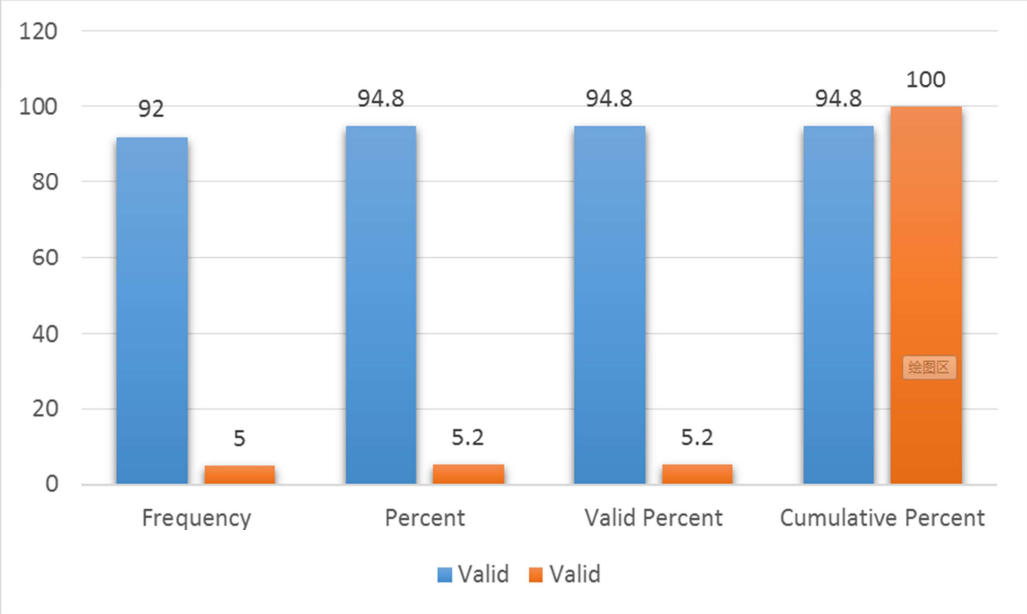

Figure 3. *Statistic of log views.*

5. Conclusion and Recommendations

At the end of this study, we actually find that there are failures and security risks that health structures encounter in the management of their data. By underestimating the permanent implementation of the IT security audit and the monitoring of the logs, these structures are clearly exposed to IT security risks. Introducing IoT can help because IoT has been widely used to link existing medical resources and provide reliable, effective and smart healthcare services [7]. We offer the following solutions.

Proposal of Solutions:

1) Integrate into their security policy the continuous and permanent implementation of the IT security audit;
2) Consider the results of the audits and apply the resulting recommendations;
3) Permanently check the logs and anticipate the implementation of decisions that can avoid risks to the structure;
4) Raise awareness and train the players in the patient data management chain.
5) Introducing technology can help reduce the risk of leak of data. Indeed a De-Identification Mechanism of User

Data in Video Systems According to Risk Level for Preventing Leakage of information in the health structures [8].

6) Others approach can be use. Indeed, Introducing Digital watermarking for data leakage detection aims to prevent the unauthorized disclosure of data by imperceptibly marking the data for each authorized user, so that the authorized user can be identified as the data leaker and be held accountable [9]. Also it is important to consider the use of hypervisor-based memory introspection for implementing data leakage detection in the health structures. The approach looks for the presence of sensitive raw data in the memory of both the client machines and the server machines, transcending the dependence of pre-existing security perimeters [10].

References

[1] DOCUMENTATION, T. P. S., & LOGICAL, C. (2005). Information technology–Security techniques–Information security management systems–Requirements.

[2] Kanatov, M., Atymtayeva, L., & Yagaliyeva, B. (2014, December). Expert systems for information security management and audit. Implementation phase issues. In *2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS)* (pp. 896-900). IEEE.

[3] Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*, *13* (1), 60-79.

[4] Ardito, C., Di Noia, T., Di Sciascio, E., Lofù, D., Pazienza, A., & Vitulano, F. (2021). An artificial intelligence cyberattack detection system to improve threat reaction in e-health. In *Proceedings of Italian Conference on Cybersecurity (ITASEC 2021)*.

[5] Mohammadi, F., Panou, A., Ntantogian, C., Karapistoli, E., Panaousis, E., & Xenakis, C. (2019, October). CUREX: seCUre and pRivate hEalth data eXchange. In *IEEE/WIC/ACM International Conference on Web Intelligence-Companion Volume* (pp. 263-268).

[6] Arasteh, A. R., Debbabi, M., Sakha, A., & Saleh, M. (2007). Analyzing multiple logs for forensic evidence. *digital investigation*, *4*, 82-91.

[7] Ray, A., & Newell, S. (2010). Exploring information security risks in healthcare systems. In *Health Information Systems: Concepts, Methodologies, Tools, and Applications* (pp. 1713-1719). IGI Global.

[8] Kim, J., & Park, N. (2022). De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information. *Sensors*, *22* (7), 2589.

[9] Gringinger, E., Schuetz, C. G., & Schrefl, M. (2021, February). Towards Informed Watermarking of Personal Health Sensor Data for Data Leakage Detection. In Digital Forensics and Watermarking: 19th International Workshop, IWDW 2020, Melbourne, VIC, Australia, November 25–27, 2020, Revised Selected Papers (Vol. 12617, p. 109). Springer Nature.

[10] Mallissery, S., Wu, M. C., Bau, C. A., Huang, G. Z., Yang, C. Y., Lin, W. C., & Wu, Y. S. (2020, October). POSTER: Data Leakage Detection for Health Information System based on Memory Introspection. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (pp. 898-900).