# IS ADOPTION OF IPSAS CONSTITUTES SUPPORT TO DIFFERENT SECURITY SYSTEMS ADOPTED IN THE LEBANON PUBLIC ACCOUNTING SECTOR

**Ali KASSEM**
*THE BUCHAREST UNIVERSITY OF ECONOMIC STUDIES, BUCHAREST, ROMANIA*
alikassem.finance@gmail.com

**IONESCU BOGDAN STEFAN**
*THE BUCHAREST UNIVERSITY OF ECONOMIC STUDIES, BUCHAREST, ROMANIA*
ionescub@gmail.com

***Abstract***

*Public accounting is one of the industry's very growing sectors.The objective is to generate a large amount of Financial information that can be further used by stakeholders to make informed decisions false information or could jeopardize the businesses involved and therefore this type of information must be Protected from external and vulnerable attacks. As the transparency and accountability of the financial Statement is very important for the trust of both the stakeholder and the investment, the security of financial information is very important for the relevance, validity and reliability of financial data.however, there is always a persistent risk of Security breaches such as attacks by brute force to obtain the information. The main focus of this paper is to examine if the adoption of the IPASS in the public accounting sector in Lebanon Support and leverage the security systems and strategies used by Lebanon's public accountants to secure financial data and financial report relevance. A quantitative methodology was used to carry out this study and a survey was conducted with a representative sample of accountants currently employed in the government sector in Lebanon. The survey questionnaire was prepared to measure the extent where recently the IPASS was adopted in public accounting security in Lebanon and also to evaluate their efficiency in data protection and to detect threats. The research carried out is likely to determine the quality of financial data protection in Lebanon's public accounting in conjunction with the application of IPASS and suggest possible solutions to enhance security. As security measures are an integral part of the IPSAS implementation process, this study contributes significantly to both the IPSAS adoption theory and the practice of aligning local accounting practices with international standards through exorbitant efforts to enhance security management in the Public Accounting Sector of Lebanon.*

***Keywords:*** *Security of information, security, leakage of information, public accounting, IPSAS, implementation of IPSAS, Lebanon*

***Clasificare JEL:*** *M41*

## 1. Introduction

At all levels, organizations and government agencies are more concerned with preparation and presenting financial statements to ensure accountability and transparency are maintained. Accountability and transparency are the key indicators that can be used to maintain confidence and honesty in both public and private organizations ' handling of public funds (Aliyu, &Balaraba, 2014). The management of the organization often stresses the challenges of corruption, non - accountability and misappropriation of funds.

In recent decades, information technology (IT) has been extremely affecting almost all gover nment and Private sectors. It has surely also played a crucial role in the services provided by the nationwide public accounting Industry. However, there is no empirical research that has been specifically done to evaluate the impacts of information Technology on the public accounting firms. Though, in order to make efficient use of information technology in the Public sector there is a dire need of evaluating it and hence this research focuses on the different security systems that are currently adopted in the public accounting sector in Lebanon.

The study will mainly focus on the firms and office, where recently large IT investments were made, primarily in the audit software and the knowledge sharing applications. The

quantitative information from the research will be analyzed to estimate the accountant's perception of different security systems and how efficient they are in detecting the threats and preventing it. The results from the analysis will indicate the significant steps that are to be taken to strengthen the IT implementation in public accounting sectors (Banker, Chang, & Kao, 2002).

There are still many challenges facing the implementation of IPSASs (international public sector accounting Standards) in Asian countries including Lebanon. According to the report by Ryan, Guthrie, & Day (2008), Lebanon is using the IPSASs system however in a much weaker form Therefore, the strategies implemented to monitor the implementation of IPSAS in Lebanon need to be enhanced. The strategies can be improved through collaboration with the competent authorities such as International Public Sector Accounting Standards Board (IPSASB) to train accountants and financial managers in Lebanon. The training will improve the efficiency of the staff using the IPSASs guidelines (Barton, 2009).

The advances in the field of information technology had a huge impact on many firms in the professional services industries of Lebanon, but perhaps the public accounting industry is the one to worry about. The public accounting industry was once considered as a slow paced and a very conservative industry, however in recent years this industry has undergone incredible changes at the turn of the era, glinted with the rapid changes in its technological environment (Elliott, 1998). The audit software as well as the other knowledge sharing applications are the most critical components of these changes. The mechanization of the audit tasks and the use of Audit software has replaced IT for the manual labor and thus the structure of the audit teams changed consequently.

Another important use of information technology in public accounting is to maneuver the advanced systems and to get the useful as well as shared knowledge from different parts of the organization. This use of information Technology has enabled the professional services that can be leveraged effectively by the human resources (Gogan, Applegate, & Nolan, 1995). Thus, with the rapid use of information technology, various researches have been conducted in the area of practitioner-oriented accounting, which discuss how to prevent the security breaches in current technology (Smith, 1997). In order to justify the use of IT in public accounting, the managers need to understand the potential benefits resulting from the investment and how these benefits can be manipulated with a typical security breach.

Though, there is a general perception of accountants that the use of information technology in public accounting can improve the firm's productivity, but they are ignorant to the fact that its use also triggers numerous vulnerabilities that are to be taken care of. The impact of IT on the firm's performance cannot be evaluated directly. The public accounting firms need to understand the threat to the information and how it can be encountered. The technology can certainly transform their work, but whether such transformation leads to productivity gain or not is dependent on the system's security (Lee & Arentzoff, 1991).

The longitudinal analysis before and after implementation of information technology is an important task to support the causality argument, which leading from IT deployment to its improvement for the firm's productivity. This is especially essential for the public accounting firm, where the use of information is one of the core competences. The aim of this research is to evaluate the accountant's perceptions on the adopted security system in Lebanon's public accounting sectors. By doing this, it can be determined that how a security breach or the improper use of a security system can impact the productivity of a public accounting firm. The empirical results from the surveys conducted in this research indicated a significant need to improve the implementation of IT security systems (Zarowin, 1994).

## 2. Literature review

Since the tremendous use of Information technology, a lot of theories have been worked upon and exhausted to study the challenges of adopting a Computerized Accounting Systems (CAS). Not only were that but numerous Technology Acceptance Model (TAM) developed to automate the system and to make it much more efficient. Some of the very famous models are the Roger's Diffusion of Innovation (DoI) model and the Unified Technology Acceptance User Theory (UTAUT) (Venkatesh, et al 2003). The Technology Acceptance Model has proven to be a very effective information systems model that has been accepted by the users.

However, any model that has been developed and is presented to the users there are two very important factors that must be heeded to. These factors are inclusive of the decision-making skills of the users about how and when they need to take the specific action. The success of any theoretical model is totally dependent on its ability to cope up in the time of crisis and to hold a secure front. Though, it is also necessary for the users to understand and the behavior of the system even before its implementation. Various models when tested usually fails to provide the required security (Juiz, Guerrero, & Lera, 2014).

For the very first time the threat to the accounting firms was realized in 2013, when about 900 of the Connecticut residents in the Fairfield County found out that the small-town accounting firm has become a prime target for the hackers and in an aftermath the tax returns were stolen directly from the firm's computers. The hacking scheme was very turbulent, yet very cleverly the selected returns that were completed but not filed were altered and then sent to the IRS in hopes of collecting the refunds even before the legitimate filers could find out about it. This incident made it clear that even the small public accounting firms are exposed to the risk of information theft and manipulation.

Though, the stolen tax returns might seem nothing but the expanse of personal information amassed by the CPA firms about the clients over many years, when leaked can be very overwhelming. This staggering information in the hands of a cybercriminal, might lead to a bigger damage inclusive of the fraud, identity theft and even the theft of tangible property. Thus, from the very smaller public accounting firms that works with the individuals as well as with the small business clients, to the international CPA firms that offers services to the world's renowned and magnanimous corporations the accounting practices of all streaks and of all sizes should take major steps in educating the accountants about cybersecurity and familiarizing them with the systems vulnerabilities (CIPFA & IFAC, 2013).

Various information technology models developed for the public accounting sectors are codependent on the security audits that improves the system compliance and can also benefit in long run. The cybersecurity professionals are now working with the accounting professionals to find the ways of preventing all sort of security threats to the data. The identify issues are dealt by using the same traditional techniques that accountants used with their clients.

The system security audits became the ground zero for preventing the vulnerable threats to the data. However, these audits are very much similar to the traditional financial audits, yet it is automated. All the checks require minimum time of the accountants, while they go through the configuration details as well as keep track of the logs and records. All the activities must then be compared to the recommended and the required settings. In case of malfunctioning, it must be reported to the notice of offending parties for correction. This is by far the accepted model of the cybersecurity, yet an orderly and a very effective procedure that fits perfectly to the regular practices of an accounting firms. Though, a recent survey of Association for Chartered Certified Accountants (ACCA) indicated that nearly half of the member of the firms periodically opts to engage in the information system security audits. Thus, this lack of concern might be damaging to the firm itself. The ACCA has thus advised the accountants to work in collaboration with the

cybersecurity professionals as well as with the other professional services to enhance the security posture of a firm.

Since the high security risk to the public accounting firms, the ACCA is currently working with the ISACA (Information Systems Audit and Control Association), which also a non-profit organization that supports the information systems security professionals and educate the ACCA members about the cybersecurity administration, analysis, audits as well as with the system structure (Brecht & Martin, 2006). Aliyu, &Balaraba (2014) stated that the need for greater accountability and transparency in government institutions handling funds and resources was heightened by the global financial crisis which led to reduced resources available for both the government and private sector

The Journal of Accountancy in 2015 conducted an interview with the three technology focused CPAs. In an interview the state of the accounting industry was clearly depicted, where it was also mentioned that the accountants, who give no importance to the system security gives no importance to the system architecture as well. Most accountants have a perception that the cybersecurity policies are only applied just in the office, thus they seem really confused on the prospect of the applications and services that are cloud-based. This is due to their unfamiliarity with the system's security features, which might pose a threat to the data. Thus, overcoming all the knowledge gaps regarding the cybersecurity is important for the accountants before they even familiarize themselves with the system.

Undoubtedly, some of the smaller firms have also become aware of the security threats and the risks. Even the Lebanese Government have made vigorous efforts to align the corporate financial reporting requirements and has made an effort to work with the International Accounting Standards (IAS). The IAS has been accepted as an international standard to be followed in all the financial statements in Lebanon. Moreover, a lot of effort is made to produce the high-quality financial reporting for the public interest entities, so that they can make an informed decision (Juiz, Guerrero, & Lera, 2014).

While IAS is an adaptive system but it is much more complicated than the small and medium size enterprise and despite implementing the international standards, there still are the loopholes and the compliance gaps of varying degrees in both the auditing and accounting practices in the firms. Though, a very minimal gap or a loophole is enlisted in the companies and the banks, but a greater gap is noticed in the public accounting firms and other companies. These loopholes are primarily due to the shortcomings in the professional education and practices in Lebanon. The main reason of this shortcoming was that when the Lebanese Association for Certified Public Accountants was established in the year 1994, the applicants who were offered a license to practice, were certified even without an examination. Also, there was no such enforcement mechanism to ensure the IAS compliance for the accountants.

In a survey conducted in 2014 by the Accounting Web, about 65 percent of the accountants indicated that the cyber threat level is high or increasing and only 14 percent of then gave an indication that they were directly involved in securing the information from vulnerabilities and other cyber threats. This pose a serious challenge for the cybersecurity professionals to overcome their shortcomings. Undoubtedly, in accounting it is a professional tribute to rigidly adhere to the rules and the formats that can be altered with time, but it can be a very challenging task to convince the CPAs as well as the firm executives to constantly update the security protocols in response to the new threats. Thus, the accounting firms becomes an easy pick for the hackers.

Though, with the target on their backs, of course the huge accounting, auditing, and other professional services inclusive of finance have exerted an ample amount of resources to strengthen their system's security as well as improve its architecture to prevent an impulsive and massive cyber thefts. But the smaller local accounting firms are not prudent enough to adapt the security system. The hackers always target the path of least resistance and the smaller firms are much of the

listed target. Also, the access to information is very easy in the tax returns, bank statements, and other legal documents (Rahman, Msadek, Jaoude, & Gielen, 2003).

Undoubtedly, the number of small-scale accounting firms is infinitesimally small in comparison to the other massive international professional services firms or the regional CPA firms. Therefore, there is a high risk of security threat and it could easily lead to the false sense of security. A lot of accountants have a perception that if there is no attention paid to their data the chances are that it won't be hacked. Though, this approach is untrue for the high-speed world of the Internet. It becomes very easy for the hackers to scan numerous smaller networks rather than scanning a few larger networks.

The knowledge of the financial position of an organization entity helps to develop future strategies and better financial judgments. The IPSASs legislations have made it easy for auditors to deliver effective audits that help to mitigate risks. IPSASs also streamline standards reporting processes hence helping to support the consolidation of all financial activities. Other benefits of IPSASs as discussed by Adejola (2012) include enabling sound financial management, enhance professionalization and access to talent, and enhance international comparability, government stability and the broader economic and social performance of an organization.

Moreover, the extent to which these threats have become automated is very shocking and has become very challenging to the information security. But all these threats can be resolved proactively, if the vulnerabilities are detected quickly and preventive steps are taken as recommended by the network administrator. The complacency and the rigidity of the system are also difficult problems that needed to be taken care of. Usually, when a market pressures increased the public accounting sector is exposed much more to these vulnerabilities and then even a small glitch causes a fortune (Juiz, Guerrero, & Lera, 2014).

The public accounting sector also allows a consumer and an accountant to connect and interact online for various decision-making advices. Consequently, there is also an involvement of the legal documents of a consumer, when these documents are submitted online, it becomes a vulnerability. Also, the use of electronic signature has increased the risk of threat to any firm. As the accounting firms take upon all the pressure of implementing the security within the systems, they sometimes do run the risk of creating more loopholes that can be further exploited.

The use of client portals and the quick deployment of the sensitive information through the contracts can rife up the vulnerability factor of an information security system. If this exploitation in the public relations sector hitting the accounting firms is not an enough motivation for the accountants, then a hit to the bottom line will be. According to the Accounting Today, most of the CPA firms are legally accountable to the Government for exposing the customer data because of a vulnerability (CIPFA & IFAC, 2013).

Moreover, the firms that still do not rely on the expertise of a cybersecurity experts are accountable to answer under a barrage of civil claims as well as the government sanctions. Also, it has become mandatory for all the accountants and professionals in the accounting industry to allocate their major resources to the structure of cybersecurity system and even have a dedicated in-house team or a contracting party with respected expertise in the field of cybersecurity (Banker, Chang, & Kao, 2002).

## 3. Methodology

This research was guided by the quantitative methodology and is characterized by testing the validity of theory on the basis of the results generated. According to the literature review the extent and impact of cyber security in the accounting practice of public institutions is dependent on various factors inclusive of the size of the organization, qualifications of the accountants, training on the use of secure systems, level of awareness, availability of the resources, audit and compliance in accordance to the policies (Brecht & Martin, 2006).

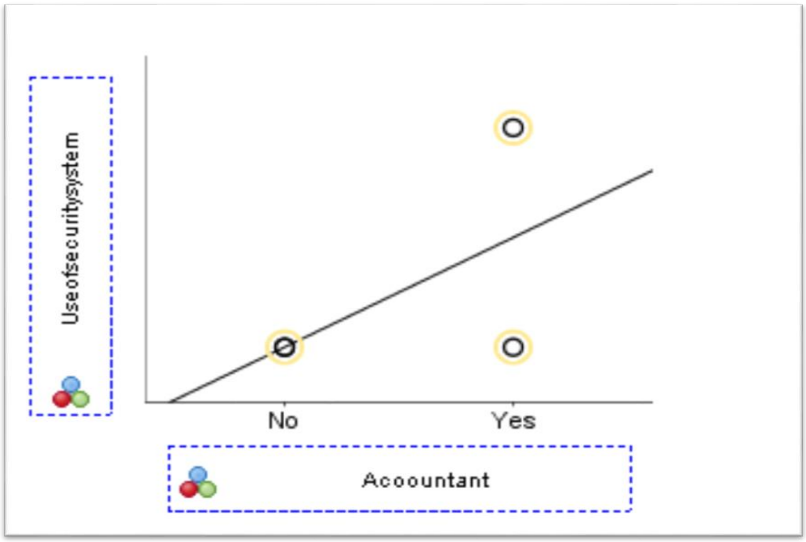
Moreover, the efficiency of the security systems is also co-dependent on the accounting practices. However, there are some accountants who still presume that a vulnerable attack on the information or data set is minimal in the public accounting sector. The quantitative analysis will allow the research to be conducted on a population that connotes an entire group of individuals, events or objects having a common, yet observable characteristic.

The data is collected using a questionnaire that was prepared to conduct this research (See Appendix I). The reason to use a questionnaire is that it covers large sample at a very low cost. However, a questionnaire is also disadvantageous because firstly it may have a low response rate, a situation whereby some of the respondents may not be willing to fill the questionnaires. Secondly, questionnaires may bring along uncontentious and dishonest replies where the target population may give wrong responses regarding the topic questions. Finally, the questionnaires lack personalization hence hidden agendas that maybe expressed through facial gestures and expressions may not be simple to realize. However, in our case, the response from the questionnaire was obtained, sampled and recorded. The sample allows to collect response from a smaller group of accountants that truly represents the bigger part of the population working in the Lebanon public accounting sector.

## 4. Results and discussions

The Survey questionnaire respondents were 100, who either worked in financial firms or in Lebanese financial government agency. The questionnaire was drafted in accordance with the research scopes. In order to evaluate the responses SPSS was used and the following graphs depicts the responses of a population representing the accountants working in the financial firms of Lebanon.

**Figure No. 1. A Graph of use of security system against accountants**

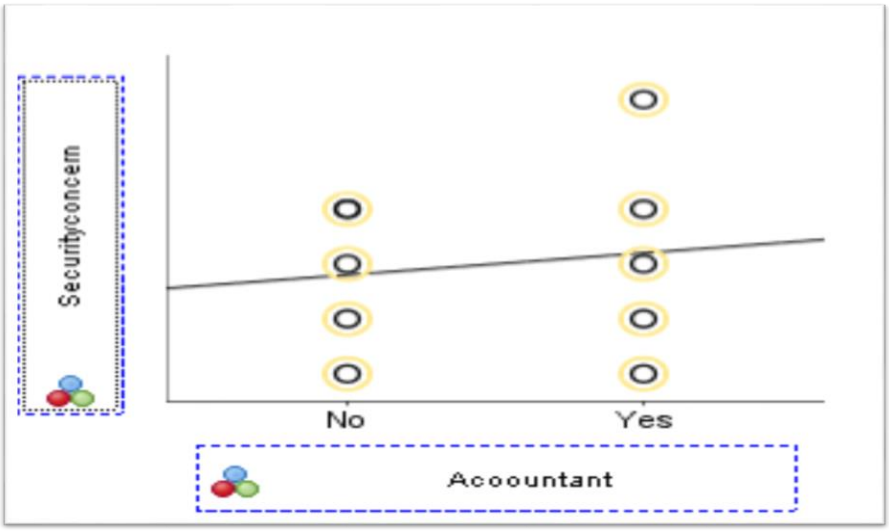



Source: Author's own research

In this scattered plot it can be seen that the majority accountants agreed on the fact that their firms use Security systems when it comes to sensitive data in public sectors. This prevents the data from falling into the hands of hackers and thus prevent loss or damage of information through cyber robbery. Furthermore, secured data lowers operational costs that might result from high expenses that might be incurred in case a security is bypassed. The so saved cost maybe used to develop more complex security authentications that will also reduce development and support time. However, there are still a number of firms that do not take steps to secure the public information,

though the number is small, but it is quite alarming. These firms tend to always be at risk of robbery and cyber terrorism, which may in return turn to them incurring high costs in case of an incident.

**Figure No. 2. A Graph plot of security concerns when the IPSAS is adopted against the accountants**.

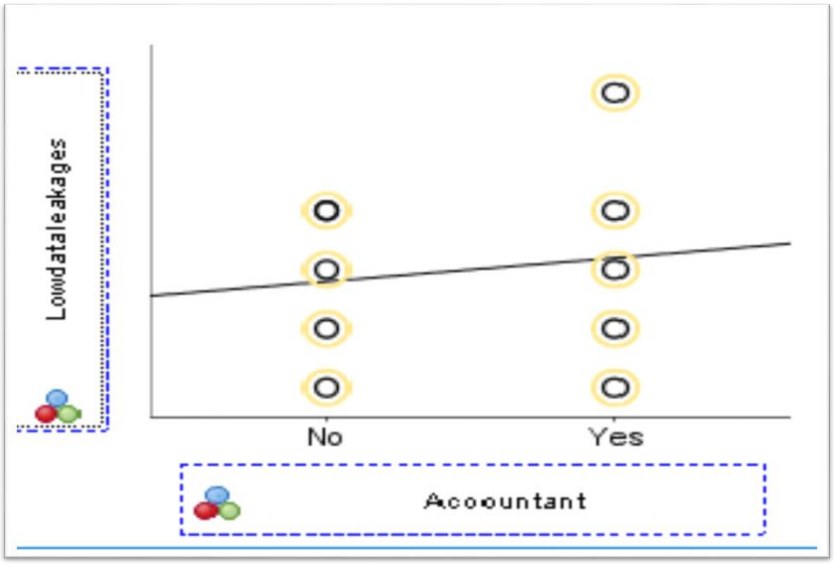



Source: Author's own research

Though the firms take duly notice of the prevailing security concern and work towards making it efficient when the company adopt the IPSAS. However, out of 100 only 59 respondents agreed that their firms take serious notice of all the security concerns and thus due to this there is a disturbing record of data leakage incidence within the firm.

According to the survey conducted, only 34% agreed upon the fact that the data leakage incidence is low in their organization when the company adopt the IPSAS, whereas 32% disagreed on the fact that the data leakage percentage is less. The remainder percentage of the respondents were neutral as depicted in the graph.

**Figure No. 3. A Graph Illustrating the Population of Accountants Experiencing Data Leakage Incidence.**




Source: Author's own research

## 5. Conclusion

The computerized accounting information system that is used by the executives' officers of government's ministries or in the departments as well as agencies have an ample amount of sensitive data that needs a proper security structure to remain unscathed. A lot of automated accounting models are proposed by the researchers that can prove to be very effective, though the implementation of such model requires a proper training that must be offered to the accountants.

The information and communication technology (ICT) have undoubtedly within the adoption of the IPSAS have transformed the firms in the professional arena, but only few accountants in the public accounting sector heed much to it. Thus, in the Lebanon public accounting sector there is a need to undergo a tremendous change at the turn of this millennium, sparked largely by the potential security threats that prevails in the world of Information Technology.

This study aided in finding out the loopholes that hinder the implementation of security within the system and the adoption of the IPSAS. Though, the government is working towards making its system efficient enough within the adoption of the IPSAS, but there is a lack of proper training and education in the accounting sector in regards to the information security structure and the full implementation of the IPSASs guidelines is still facing a lot of barriers. The key barriers that have come out clearly from the study findings included lack of government support, a high cost of implementation, resistance to change and lack of better understanding of the significance and operation of the IPSASs tool. Though there is still a need to educate the Lebanese accountants, where information security is concerned.the government should strengthen the auditing firms across Lebanon to ensure that they are complying with IPSASs Provisions. This issue causes a challenge for the public sectors to excel and improve in the future.

## 6. Bibliography

[1] **Aliyu, A. & Balaraba, A.** (2014). IPSASs and financial and financial reporting in Nigeria: Answer to implementation questions. Journal of Economics and Finance (IOSR – JEF), 6(6), 28–32.

[2] **Applegate, L. (2019). Lynda M. Applegate**- Faculty & Research - Harvard Business School.

[3]**Banker, R. D., Hsihui Chang, & Yi-ching Kao.** (2002). Impact of Information Technology on Public Accounting Firm Productivity. Journal of Information Systems, 16(2), 209–222.

[4]**Barton, A. (2009).** The use and abuse of accounting in the public sector financial management reform program in Australia. ABACUS, 5(2), 221-248.

[5]**Brecht, H. D., & Martin**, M. P. (1996). Accounting Information Systems: The Challenge of Extending Their Scope to Business and Information Strategy. Accounting Horizons, 10(4), 16–22.

[6]**CIPFA, & IFAC.** (2013). Good Governance in the Public Sector—Consultation Draft for an International Framework

[7]**Elliott, R**. K. (2000). Who Are We As a Profession--and What Must We Become? Journal of Accountancy, 189(2), 81–85.

[8]**Juiz, C., Guerrero, C., & Lera**, I. (2014).Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks

[9]**Lee, J. Y., & Arentzoff, S**. (1991). The productivity factor: justifying your computer purchase.

[10]https://www.hbs.edu/faculty/Pages/print-profile.aspx?facId=6411

[11]https://doi.org/10.2308/jis.2002.16.2.209

[12]http://165.193.178.96/login?url=http%3a%2f%2fsearch.ebscohost.com%2flogin.aspx%3fdirect%3dtrue%26db%3dbth%26AN%3d9707141997%26site%3deds-live

[13]http://www.ifac.org/system/files/publications/files/Good-Governance-in-the-Public-Sector.pdf

[14]http://165.193.178.96/login?url=http%3a%2f%2fsearch.ebscohost.com%2flogin.aspx%3fdirect%3dtrue%26db%3dbth%26AN%3d2761270%26site%3deds-live.
[15]http://www.ifac.org/system/files/publications/files/Good-Governance-in-the-Public-Sector.pdf.
[16]https://www.thefreelibrary.com/The+productivity+factor%3a+justifying+your+computer+purchase.-a010737508