

Sarbanes-oxley act: advantages and disadvantages



**ASSIGN
BUSTER**

Discuss the strengths and weaknesses of the Sarbanes-Oxley (SOX) Act and describe how an IT department can meet the challenge of implementing SOX compliance

Over the past ten years we have been exposed to a series of financial scandals. The effect has been catastrophic and society has required regulation to restrain corruption. In 2002, the USA senator Paul Sarbanes and Representative Mike Oxley sponsored the Public Company Accounting Reform and Investor Protection Act. It is generally called the Sarbanes-Oxley (SOX) Act and was put in place in order to regulate the accountability of financial reports and prevent risks occurrence. However, the deployment of SOX compliance costs a lot of money, resources and efforts. It not only affects the finance department, but also the information technology (IT) department. The risk prevention and cost concern of SOX Act will be described in the first paragraph; the pros and cons of process control, documentation and responsibility will be discussed in the next; the strengths and drawbacks of security control will be indicated after that; then the challenge of an IT department for SOX compliance will be examined. Finally, a case study on the Enron scandal will be introduced. This essay will help prove that the SOX system is worth the price despite certain drawbacks and discuss how an IT department meets the compliance.

It is worth preventing potential risks by effectively performing the SOX regulation in spite of extra costs and workload. To begin with, SOX Act provides a guideline of internal control for financial statement to prevent any potential risk, all the financial events and accounting activities will be managing by this mechanism. Thus, the financial statements would be more accurate and reliable (Anand 2006: 2). In addition, through regular internal

and external auditing to ensure there has no unscrupulous behaviors in the financial operations. Consequently, the potential risks can be minimized and unethical behaviors can be prevented and deterred. However, the finance and IT departments must budget the expenditure of SOX implementation at the beginning and also need to pay external accounting firms for regular examinations every year. The estimation of its cost was around USD 91, 000 with an extra 383 man hours in 2003, and the cost is still increasing every year (Jahmani and Dowling 2008: 59). Staffs have an increased workload by collaborate with consultants for the auditing. Those employees not only have to document routine activities, but also need to prepare a lot of evidences for auditors' investigation. Although employees may suffer through these additional tasks, some unexpected benefits will be gained from them as well.

The transparency of documentation gives a company more integrity even though some process changes are required. The standard operating procedure (SOP) of each department must be documented, especially for those operations involve to financial activities and SOX compliance. Namely, the internal or external auditors will investigate any potential risk of process control according to the documentation. It is thought that the establishment of SOP and documentation would be an advantage to companies, because it demonstrates the system of a company and employees are easy to follow, and it also improves the effectiveness and efficiency of business process. In addition, the segregation of duties is also a critical control point to the SOX compliance for the risk prevention (Anand 2006: 53). Employees are required to request accounts to the system administrator according to their responsibility, and other colleagues are disallowed to process information

systems through other people's system accounts. Thus, every single detail is filed into the information system with regular backup solutions. It provides the traceability for auditors investigating any suspected issues. Conversely, companies may need to change business process flow and modify related system flow in order to align with SOX Act guideline. They must pay extra costs of business process re-engineering and IT staffs must enhance information system to meet those requirements as well.

The regulation of security control will avoid inappropriate behaviors happening although employees may feel frustration. The IT department performs a very important role to assist and reduce the effort of manual jobs. However, they usually have more authorities in system to support user needs. For this reason, IT members are also divided into different roles, and those roles are usually separately assigned into server, database, security and application systems. Every change and modification must be approved and documented into the system. Moreover, those changes must be regularly reviewed by the management team in the change management meeting (Sentt and Gallegos 2009: 408). Thus, it will be more safety and the risk of system change can be diminished. In sum, employees have clear understanding of their roles and their performance can be easily traced from the information system. Potential risks can be also minimized by the restriction of system design and security control. Despite this benefit, more staffs may need to be hired to prevent the conflicts of job duties, because employees cannot validate the rule of segregation of duties. Finally, owing to those complicated restrictions of SOX compliance regulation, employees may feel frustrate of against rules. They may prefer focusing on their routine

tasks rather than extending their capability to involve another area because of risks taken.

IT department often plays an important role of implementing SOX compliance for the information system perspective. There are some approaches suggested for an IT department to cope with the challenge of SOX compliance. To begin with, a sophisticated information system is fundamental in implementing SOX compliance. The Enterprise Resource Planning (ERP) system automatically calculates financial reports and its operations usually can meet Sarbanes-Oxley Act requirements (Pathak 2005: 72). Next, the system change and program version control are also mandated. Therefore, the introduction of a change management system would be helpful for executing these changes. In addition, cross check of those changes would help companies prevent any unexpected disaster as well as some frauds in purpose. Furthermore, system logs, backup solutions and security controls are also critical for an IT department meeting the criteria of SOX implementation. Ultimately, documentation is a basic element for the success of SOX compliance implementation. Therefore, system manuals, user manuals, transaction logs, security control sheets, schedule jobs and change request logs must be archived and categorized in the file system. In short, as long as IT department follows above guidelines, then it will not be difficult to meet the challenge of implementing the SOX compliance.

Let us now look at the Enron scandal, a crucial example not least because of its impact on the USA government and society. The aftershocks were felt globally. Enron was an energy company which supplied electricity and gas in

<https://assignbuster.com/sarbanes-oxley-act-advantages-and-disadvantages/>

the USA. This company was also providing bandwidth service, paper and metal commodities. However, those investments seemed not successful and profitable. Enron therefore had created a lot of overseas special purpose entities for hiding Enron's losses on their financial reports, and it had also created the illusion of profitability which was actually losing money. Besides, Enron's audit firm Arthur Andersen had a long term relationship and it assisted Enron to hide losses by destroying related documents. Eventually, their conspiracy was exposed to society due to revelation of a huge amount of undisclosed losses – USD 586 million. The stock price had a dramatic fall from approximately USD 90 dollars to 30 cents. Finally, Enron was filed bankruptcy in 2002 (Welytok 2006: 26). People should learn the harmful from this incident, particularly the US government and the entire corporate must prevent such kind of scandal occurring again. Therefore, the implementation of SOX Act would be a good approach to curb corruption. The evidence shows that implementing and sustaining SOX compliance could minimize fraud or crime risk up to 95 per cent of a company, if that company performs it appropriately and effectively (Anand 2006: 196). It demonstrates the significance and effectiveness of SOX compliance.

In conclusion, there are several advantages and disadvantages for implementing SOX compliance in companies. First, financial reports would be more transparent and reliable through auditing controls, and potential risks will be reduced. Next, both companies and employees will benefit from the creation of documentation. Because it meets SOX compliance and helps employees understand the business processes. After that, it is more safety for the restrictions of system account and authority, and those possible

swindles would be minimized. Conversely, there are some disadvantages of SOX compliance to companies. First, SOX compliance implementation will cost a lot of expense, and companies have to budget for SOX auditing every year. In addition, the processes change of a company is inevitable to conform to the guideline. Furthermore, employees may lose their enthusiasm for job due to the limitations of SOX Act, employees would become frustrated of involving the other areas. Finally, some strategies are advisable for IT department implementing the SOX compliance. For instance, a sophisticated ERP system can be easier to adapt the change of SOX compliance implementation; change management and version control must be under controlled; preparing all documentations as possible as you can. Above all are basic elements for the success of SOX compliance implementation.

Reference list:

Anand, S. (2006) Sarbanes-Oxley guide for finance and information technology professionals. New Jersey: John Wiley

Jahmani, Y. and Dowling, W. (2008) ' The impact of Sarbanes-Oxley Act' Cluteinstitute-Onlinejournal [online] 6(10), 57-66. Available from [26 August 2010]

Pathak, J. (2005) Information Technology Auditing – An Evolving Agenda. New York: Springer

Sentt, S. and Gallegos, F. (2009) Information technology control and audit(3dn). Florida: Taylor & Francis

Welytok, G. (2006) Sarbanes-Oxley For Dummies. Indiana: Wiley