CHAPTER V. CONCLUSION AND RECOMMENDATION

PT Avrist Assurance (or was PT Asuransi AIA Indonesia) was the first time implementing SOX compliance in 2006. The SOX compliance was started by defining the IT internal control areas.

To define the IT internal control needed to be assessed, IS audit control areas defined by ISACA was used. They are : physical/environmental review, application software review, system administration review, network security review, business continuity review and data integrity review.

After defining the internal control areas, IT compliance officer can start to assess the control in each area. The assessment can be started by assessing the risk and create the “what could go wrong” checklist with the severity value of each item.

After assessment were made, the un-comply items should be remediated. At Avrist, after the assessment period, the remediation process was finished 1 year after. Thus, on 2007, when external auditors were come to audit, only some issues founded. And Avrist immediately settle a remediation action for the findings. In 2008 internal auditors were come and they just found only 1 minor item from the audit process.

It then can be concluded that if the internal control areas of SOX compliance has been determined and assessed, IT management can monitor IT operations control more easily. It is shown from the audit report in 2007 and 2008 that only some findings were reported as the IT control gap.

PT Avrist Assurance (Avrist) had implemented SOX compliance through the IT organization and Avrist also had maintaining its IT compliance activity from year 2006 until 2008. From the audit activities from those years, founded that there are recurrence finding on user access control for applications. Thus, Avrist should have more protection on user access control for applications. because

Lack of control in user access may cause possibilities for users to input the wrong data, such as transaction date, transaction amount or transaction type and still being processed in the systems. This condition may lead to miscalculation or possibility of fraud risk and financial statement misstatement.

If the compliance system is in place, the management can freely adapt any strategy to the company, the company also can avoid the risk of data intrusion, and fraudulent access to company's financial data. Other benefits are : low level of user complaint, the company become more credible for its customers because all of the systems already standardized. The company also will have its data or information availability, confidentiality and integrity.

The company can easily adapt to a new system because Avrist already has the culture of being compliance, the cost for management to change a system is less than if the company hasn't implement any compliance.

It's been 4 years since the first SOX implementation in Avrist. To make sure a good compliance in IT activities, it is better to run the SOX compliance assessment regularly. By having compliance IT operations and having the IT operation areas being control, company can reduce the financial problems due to IT activities.