Journal of Applied Engineering and Technological Science
Vol 1(2) 2020 : 124-135

ACADEMIC INFORMATION SYSTEM SECURITY AUDITS USING COBIT 5 FRAMEWORK DOMAINS APO12, APO13 AND DSS05

Yoga Megasyah[1], Adi Arga Arifnur[2]
Universitas Nasional Pasim[1], Universitas Andalas[2]
yoga_m@pasim.ac.id[1], adiargaarifnur@it.unand.ac.id [2]

ABSTRACT

Academic information system in an institution is very important for the administration of lectures. The fore need for a system security audit so that the administration runs without obstacles. This audit can be carried out using the COBIT 5 framework, in this research an information security audit was carried out on academic information security. by focusing on the APO12 (Manage Risk), APO13 (Manage Risk), and DSS05 (Manage Security Service) domains. The stages in this research are initiation, planning the assessment, data collection, data validation, process attribute level and reporting the result. The results of this research note that the ability level of APO12 is at level 1, APO13 at level 2 and DSS05 at level 2, which means that the institution has carried out and implemented the information technology process and achieved its objectives. To reach level 3 some recommendations are given to cover the gaps that have been determined in the APO12, APO13 and DSS05 processes.

Keywords : *Information System Academic, COBIT 5, APO12, APO13, DSS05*

1. INTRODUCTION

Information technology is developing very rapidly so that it can facilitate in a variety of activities ranging from industrial and individual activities. Current technology is utilized to make it easier to do work, which previously was done manually now can be done more efficiently, effectively and thoroughly so as to reduce some of the errors caused by human error factors.

Information system security is a major problem for companies, organizations and governments. Information System Security in the Information and Communication Technology (ICT) era is very important (Ciptaningrum et al., 2015). Some of the problems are such as the evaluation of the level of maturity of the system security has not been done, the lack of commentary on reports, guidelines and SOP (Standard Operational Procedure) regarding policies related to information system security. For this reason, it is necessary to evaluate the maturity of information system security to ensure the continuity and business processes that exist so that they can provide improvements that improve the security of information systems that already exist today (Aritonang, 2018).

The selection of COBIT 5 domains for the most important corporate security can focus on APO12, APO13, and DSS05 (Greene & CISSP, 2015). Information Systems Audit can be carried out using the COBIT 5 framework (Matin et al, 2018). APO13 is one of the domains in COBIT 5 which contains the process of defining, operating and controlling the system implemented by the company to manage the security of its information. This process aims to maintain the incidence and impact of information security incidents that cannot exceed the level of risk determined by the company. As for the case that is used the Universitas Majalengka academic information system. Higher Education in Indonesia does not yet have a specific model or framework for auditing Academic Information Systems (Maria & Haryani, 2011).

Universitas Majalengka is an institution engaged in education is an example of a company that utilizes the development of computer technology that is the basis for the application of real applications of communication media and corporate data processing. In this institution, it continues to develop its information system to support all existing activity processes to be more effective and efficient.

2. LITERATURE REVIEW

Auditing is a systematic process for obtaining and evaluating evidence objectively about assertions about activities and events to match these assertions with established criteria (Messier *et al*, 2014). Evaluation to find out how the level of conformity between the application of information systems with established procedures and know whether an information system has been designed and implemented effectively, efficiently, and economically(De Haes, et. al., 2013).

Factors driving the importance of information system control and auditing can be seen in Figure 1.

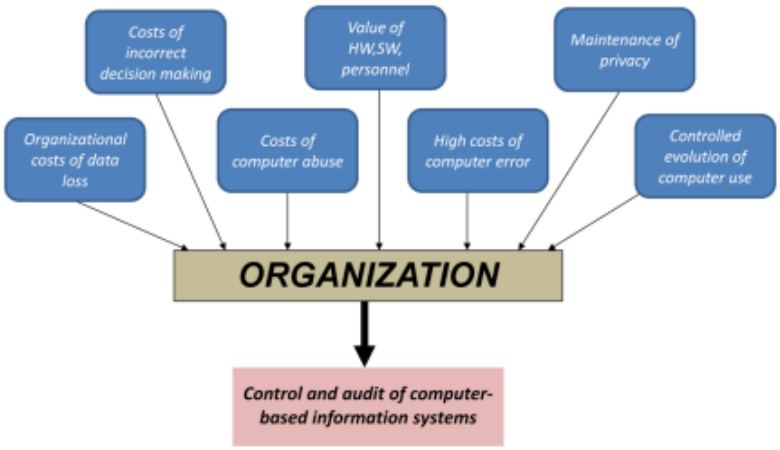

Fig. 1. Factors Influencing Organizations for Control and Audit
Source: (Weber, 1999)

IT audit activities and control there are 4 objectives of Information Systems Audit as shown in Figure 2.

Fig. 2. IS/IT Audit Purpose
Source: (Weber, 1999)

COBIT is a standard guide to information technology management practices and a collection of best practices documentation for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues(Mangalaraj, et. al., 2014). COBIT 5 generally has 5 basic principles as shown in Figure 3.

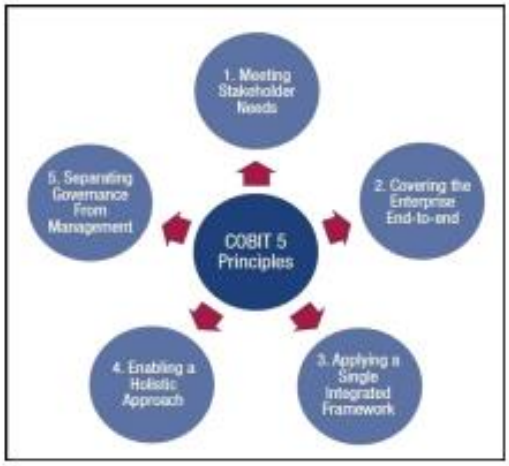

Fig. 3. Five Principles of COBIT 5
Source: (ITGI COBIT 5, 2012)

The flow of goals in COBIT 5 is a mechanism for translating stakeholder needs into specific objectives at each level and every area of the organization in supporting the organization's main objectives and meeting stakeholder needs, and this effectively supports the alignment between organizational needs and IT solutions and services. COBIT 5 priority flow goals can be seen in Figure 4.

Fig. 4. The flow of goals COBIT 5
Source: (ITGI COBIT 5, 2012)

COBIT 5 contains a process reference model that determines and explains in detail the governance and management processes. The model represents all the processes commonly found in companies related to IT activities and provides the model as an easy-to-understand reference in IT operations and by business managers, reference model can be seen in Figure 5.

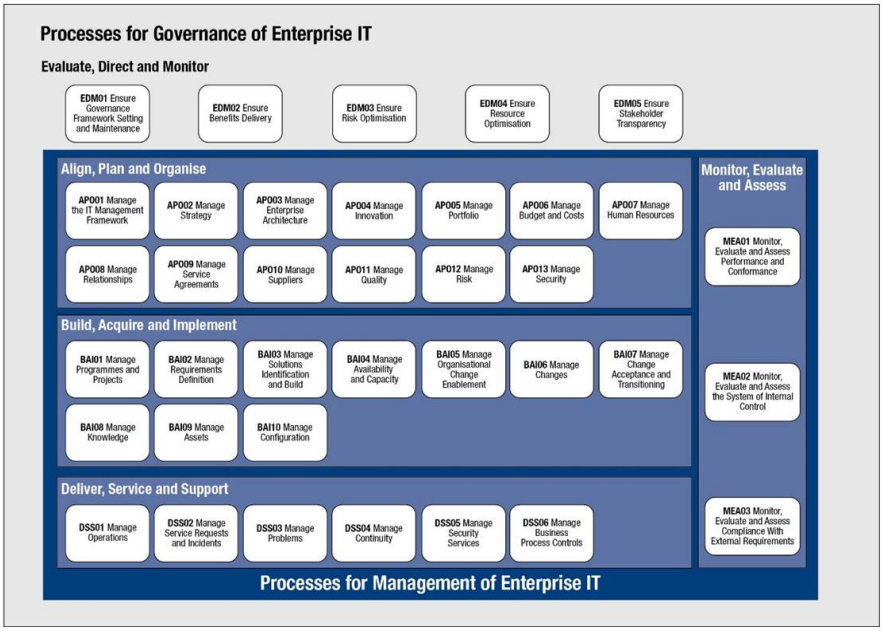

Fig. 5. Process Reference Model in COBIT 5
Source: (ITGI COBIT 5 PAM, 2013)

The COBIT 5 framework, specifically the APO (Align, Plan, and Organize) domain in the APO13 (Manage Security) process domain, can assist companies in auditing information governance, especially in evaluating the maturity level of information system security in the company. Define, operate and oversee systems for information security management(De Haes, et. al., 2020). The purpose of the process is to keep the impact and events from incidents within the limits of the risks that the company has received. The subprocesses on APO13 are as follows:

a. APO13.1, Building and Maintaining an ISMS
b. APO13.2, Define and Manage Information Security Handling plans.
c. APO13.3, Oversee and Review the Information Security Management System.

Data must be considered in risk analysis. The most important thing is the impact on the company, estimating the possibility of different threats and identifying reducing controls. APO12.01. Stakeholders must be kept informed through the articulation of risk status including the worst possible risks and the most probable scenario APO12.04. Portfolio risk management must be defined and maintained to control activities, manage, avoid and prevent or transfer APO12.05. Responses to risk events must be timely and effective based on the formal testing plan APO12.06. Such a plan must be prepared and maintained and tested periodically to respond to incidents that can affect business operations.

This service and support (DSS) process includes technical security controls to maintain the most critical, vulnerable and sensitive resources including information or data, networks and infrastructure. Specific practices that shape the security of governance follow the service process. protection against malwares (viruses, worms, spyware, scanning tools, remote access tools).

3. RESEARCH METHODS

Methodology is a determining factor for the benefits of research, and therefore the role of research is very important in writing scientific papers. Research methodology is a work step that needs to be done so that research can be a reference. The following framework used in this study can be illustrated as shown in Figure 6.

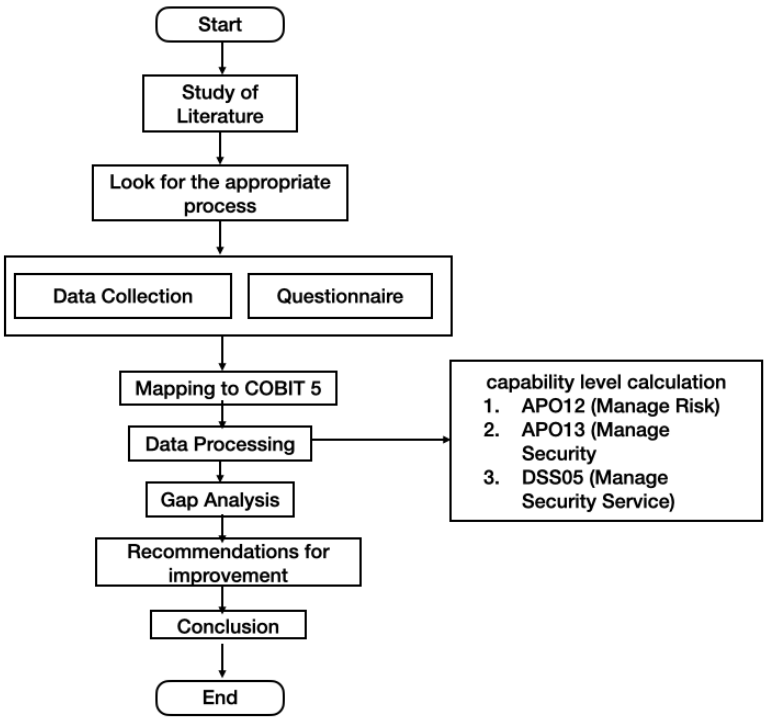

Fig. 3. Research Flow

The research methodology steps in Figure 3 are explained as follows:

Study of Literature

Literature study conducted by the author is by searching various written sources, whether in the form of books, archives, magazines, articles and journals, or documents that are relevant to the problem under study. So the information obtained from the literature study is used as a reference to strengthen the existing arguments about COBIT 5.

Look for the appropriate process

The activity carried out at this stage was to study the history and general description of Universitas Majalengka. This was done based on the initiative before the evaluation process began, as well as direct observation and interviews with stakeholders.

Data collection

Collecting data to support the evaluation of the evaluation process, as a stage in collecting data is collecting data to estimate internal control.

Questionnaire

Distributing questionnaires to the parts involved in system security at Universitas Majalengka.

Mapping to COBIT 5

Activities carried out at this stage are to do mapping based on research objects. This is done so that the assessment is appropriate and as needed in the assessment of process capability with the COBIT 5 Process Assessment Model.

Capability level calculation

The activities carried out at this stage are evaluating each process that has been carried out, mapping the process to be assessed with the aim of obtaining measurement results at the level and achieving appropriate evidence in the field based on the COBIT 5 Process Assessment Model.

Gap analysis

Gap analysis is used to determine what steps need to be taken to move from current conditions to desired conditions or desired future conditions. Done to measure levels in the APO12, APO13 and DSS05 domains.

Recommendations for improvement

This step is the output of the results of the thesis research which is useful in elaborating recommendations based on the assessment of the COBIT process which is certainly adjusted to the needs of Universitas Majalengka.

Conclusion

Provide conclusions from the results of the audit using the COBIT 5 framework with APO12, APO13 and DSS05 domains.

4. RESULTS AND DISCUSSIONS

Mapping RACI Diagram

For more valid calculations, it must be determined in advance the parts at Universitas Majalengka which are responsible for the existing processes. The RACI diagram can be seen in Table 1.

Table 1 – Mapping Result Respondents

Respondent	Amount	Scope	The process involved
Head of IT	1	IT	APO12, APO13, DSS05
Head of HRD	1	HRD	APO12, APO13, DSS05
Head of Finance	1	Finance	APO12, APO13, DSS05
Head of Planning	1	Planning	APO12, APO13, DSS05
Data & Information Division	1	IT	APO12, APO13, DSS05
Network Division	1	IT	APO12, APO13, DSS05
Development System Division	1	IT	APO12, APO13, DSS05
System Security Division	1	IT	APO12, APO13, DSS05
Academic Information System Users	23	Academic	APO12, APO13, DSS05

APO12 Process (Manage Risk)

The results of the distribution of questionnaires for the APO12 Manage Risk domain distributed to 31 respondents at Universitas Majalengka which covered all information system users and information system managers obtained data as shown in Table 2.

Table 2 – Tabulate the results of the APO12 Domain Level 0 and Level 1 questionnaires

No	Question	Yes	No	Average (%)
1	Is there a risk management application at Universitas Majalengka?	31	0	**100**
2	Have IT related risks been identified, analyzed, managed and reported?	28	3	**89**
3	Is there a current and complete risk profile?	25	6	**80**
4	Are all significant risk management actions managed and controlled?	23	8	**73**
5	Are risk management actions carried out effectively?	20	11	**64**

After obtaining the results of the questionnaire which can be seen in Table 2, the results are then submitted to the COBIT 5 Self-Assessment Guide in Table 3.

Table 3 – APO12 Self-Assessment from the Results of Questionnaire Level 0 and Level 1

APO12	***Manage Risk***						
	Purpose	Integrate enterprise IT related risk management with overall ERM and balance the costs and benefits of managing IT related company risks.					
	Assess whether the following outcomes are achieved.	**Criteria**	**Score (%)**	N (0-15%)	P (15% -50%)	L (50% - 85%)	F (85-100%)
Level 0 Incomplete	**The process is not implemented or fails to achieve its process purpose.**	Is there a risk management application at Majalengka University?	100				100
Level 1 Performed	**PA 1.1 The implemented process achieves its process purpose.**	APO12-O1 IT-related risk is identified, analyses, managed and reported.	89			76	
		APO12-O2 A current and complete risk profile exists.	80				
		APO12-O3 All significant risk management actions are managed and under control.	73				
		APO12-O4 Risk management actions are implemented effectively.	64				

The results of the calculation of scores in the APO12 domain (Manage Risk) for level 0 obtained a value of 100% which means that the process has been carried out, then an assessment of the level 1 capability is carried out. 76%, it shows that the process in the APO12 Manage Risk domain for Level 1 is in the L or Largely Achieved category, meaning that for level 1 the APO12 domain means that the process at level 1 has been largely implemented and there is a large proportion of evidence of achievement. Because the value obtained at level 1 APO12 domain averaged 76%, the authors did not continue the assessment to level 2 because to continue the assessment to level 2 the value that must be obtained at level 1 is between 85% - 100%. For the APO12 domain the capability level obtained is at level 2 or Performed Process.

APO13 Process (Manage Security)

The results of the distribution of questionnaires for the APO13 Manage Security domain were distributed to 31 respondents at Universitas Majalengka which covered all information system users and information system managers obtained data as shown in Table 4.

Table 4 – Tabulate the results of the APO13 Domain Level 0 and Level 1 questionnaires

No	Question	Yes	No	Average (%)
1	Is there a system security application at Universitas Majalengka?	31	0	**100**
2	Is the security system that has been implemented in accordance with the requirements of Universitas Majalengka?	26	5	**83**
3	Is there a plan and internal communication at Universitas Majalengka related to the implementation of system security?	30	1	**96**
4	Is the information system security solution implemented in all divisions of Universitas Majalengka?	27	4	**86**

After obtaining the results of the questionnaire which can be seen in Table 4, the results are then submitted to the COBIT 5 Self-Assessment Guide in Table 5.

Table 5 – APO13 Self-Assessment from the Results of Questionnaire Level 0 and Level 1

APO13	***Manage Security***						
	Purpose	Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.					
	Assess whether the following outcomes are achieved.	**Criteria**	**Score (%)**	N (0-15%)	P (15% -50%)	L (50% - 85%)	F (85-100%)
Level 0 Incomplete	**The process is not implemented, or fails to achieve its process purpose.**	Is there a security system application at Universitas Majalengka?	100				100
Level 1 Performed	**PA 1.1 The implemented process achieves its process purpose.**	APO13-01. Is the security system applied in accordance with the requirements of Universitas Majalengka?	83				88
		APO13-O2 A security plan has been established, accepted and communicated throughout the enterprise.	96				
		APO13-04. Is the information system security solution implemented throughout the Universitas Majalengka division?	86				

The results of the calculation of the score on the domain APO13 (Manage Security) for level 0 obtained a value of 100% which means the process has been carried out, then an assessment of the level 1 capability is carried out. 88%, it shows that the process in the APO13 Manage Security domain for Level 1 is in the F or Fully Achieved category, meaning that for the level 1 APO13 domain there is complete and systematic proof of approach, full achievement

of the attributes defined in the assessment process, no weaknesses, which significant related attributes in the assessment.

DSS05 Process (Manage Security Services)

The results of the distribution of questionnaires for the DSS05 Manage Security Services domain were distributed to 31 respondents at Universitas Majalengka which covered all information system users and information system managers obtained data as shown in Table 6.

Table 6 – Tabulate the results of the DSS05 Domain Level 0 and Level 1 questionnaires

No	Question	Yes	No	Average (%)
1	Are there actions to minimize the business impact of operational information security vulnerabilities and incidents?	28	3	**89**
2	Do network and communication security meet business needs?	26	5	**83**
3	Is information processed, stored and transmitted by endpoint devices protected?	27	4	**86**
4	Can all users be uniquely identified and have access rights according to their business role?	26	5	**83**
5	Have any physical measures been implemented to protect information from unauthorized access, damage and interference when processed, stored or sent?	28	3	**89**
6	Is electronic information really secure when stored, sent or destroyed?	30	1	**96**

After obtaining the results of the questionnaire which can be seen in Table 6, the results are then submitted to the COBIT 5 Self-Assessment Guide in Table 7.

Table 7 – DSS05 Self-Assessment from the Results of Questionnaire Level 0 and Level 1

DSS05	***Manage Security Service***						
	Purpose	Minimize the business impact of operational information security vulnerabilities and incidents.					
	Assess whether the following outcomes are achieved.	**Criteria**	**Nilai (%)**	N (0-15%)	P (15% -50%)	L (50% - 85%)	F (85-100%)
Level 0 Incomplete	**The process is not implemented, or fails to achieve its process purpose.**	At this level, there is little or no evidence of any achievement of the process purpose.	89				**89**
Level 1 Performed	**PA 1.1 The implemented process**	DSS05-01 Does network and communication security meet business needs?	83				**87**

DSS05	*Manage Security Service*						
	Purpose	Minimize the business impact of operational information security vulnerabilities and incidents.					
	Assess whether the following outcomes are achieved.	**Criteria**	**Nilai (%)**	N (0-15%)	P (15% -50%)	L (50% - 85%)	F (85-100%)
	achieves its process purpose.	DSS05-02 Is information processed, stored and transmitted by endpoint devices protected?	86				
		DSS05-03 Can all users be uniquely identified and have access rights according to their business role?	83				
		DSS05-04 Have physical measures been implemented to protect information from unauthorized access, damage and tampering when processed, stored or sent?	89				
		DSS06-05 Is electronic information really secure when it is stored, sent or destroyed?	96				

The results of the score calculation in the DSS05 domain (Manage Security Service) for level 0 obtained a value of 89% which means that the process is in the F or Fully Achieved category, then an assessment is carried out at the level 1 capability level. From the questionnaire calculation results for the DSS05 domain the average value is obtained - the level 1 capability assessment is 87%, it shows that the process in the DSS05 domain Manage Security Service for Level 1 is in the F or Fully Achieved category meaning that for level 1 the DSS05 domain has complete and systematic proof of evidence, full achievement of the attributes defined in the assessment process, no. there are weaknesses, which are significant in terms of attributes in the assessment.

Analysis of Results of Academic Information System Performance Measurement with COBIT 5 Process Assessment Model (PAM)

Based on the results of the questionnaire for the measurement of the APO12, APO13, and DSS05 domains, the results obtained are shown in Table 8.

Table 8 – Achievement of the COBIT Process Level 5

No	Process Name	Target Level	Current Level	Gap
1	APO12 – *Manage Risk*	3	1	2
2	APO13 – *Manage Security*	3	2	1
3	DSS05 – *Manage Security Services*	3	2	1

Based on the results obtained from each domain, it is found that the average capability value for the APO12, APO13, and DSS05 domains at Universitas Majalengka is at level 1 and

2, at this stage the company has run and implemented the information technology process and achieved its objectives, there is also a planning, evaluation and adjustment process in order to obtain better process results, from the results of these achievements graphs are made for the achievement of the APO12, APO13, and DSS05 domains as follows:

Fig. 4. Graph of Achievement of the COBIT Process 5

5. CONCLUSION

Based on the results of the analysis of academic information systems using the COBIT 5 framework APO12, APO13, and DSS05 domains, it can be concluded that the application of academic security information systems is at the capability level with an average of level 2, with 1 process detail, namely APO12 at level 1 while APO13 and DSS05 are at level 2. Components that need to be adjusted to be adequate for the purpose of academic information system security are the need for careful planning for system security and IT infrastructure renewal. The main priority of concern in the security of academic information systems at Majalengka University is the improvement of information systems security risk management.

REFERENCES

Aritonang, i. J. (2018). Audit keamanan sistem informasi menggunakan framework COBIT 5 (apo13). *Information technology engineering journals*, *3*(2), 5.

Ciptaningrum, d., nugroho, e., & adhipta, d.(2015). Audit keamanan sistem informasi pada kantor pemerintah kota yogyakarta menggunakan cobit, *5*, 10.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307-324.

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). COBIT as a Framework for Enterprise Governance of IT. *In Enterprise Governance of Information Technology* (pp. 125-162). Springer, Cham.

Greene, F & CISSP (2015). *Selected COBIT 5 Processes for Essential Enterprise Security*. ISACA.

ISACA. (2013). COBIT Process Assessment Model (PAM): Using COBIT 5, Rolling Meadows, United State of America.

IT Governance Institute (ITGI), ISACA. (2012). COBIT 5 Enabling Processes. United State of America.

Mangalaraj, G., Singh, A., & Taneja, A. (2014). IT governance frameworks and COBIT-a literature review.

Maria, e., & Haryani, e. (2011). *Audit model development of academic information system: case study on academic information system of Satya Wacana*. *Journal of arts, science & commerce*, *ii* (2 april 2011), 13.

Matin, i. M. M., arini, a., & wardhani, l. K. (2018). Analisis keamanan informasi data center menggunakan cobit 5. *Jurnal teknik informatika*, *10*(2), 119–128. Https://doi.org/10.15408/jti.v10i2.7026

Messier, et al. (2014). *Evaluasi Kinerja SDM*. Cetakan Ketujuh. Bandung: PT. Refika Aditama.

Weber, Ron. (1999). *Information Systems Control and Audit.* 2nd edition. Prentice Hall Inc, New Jersey.