JOURNAL OF SOCIAL SCIENCE

Printed ISSN: 2720-9938
Electronic ISSN: 2721-5202

jsss.co.id

AUDIT OF ATTENDANCE INFORMATION SYSTEM WITH FINGERPRINT USING COBIT 4.1 FRAMEWORK AT PT DSN

Alda Tasya Salsabilla*, Fitri Risca Amrizal Amelya, Rifky Ahmad Sururi, Rochmat Setiyawan
Faculty of Information Technology, Universitas Bina Sarana Informatika, Tangerang, Banten, Indonesia
Email: aldatsp27@gmail.com*

ARTICLE INFO

Date received : June 30, 2022
Revision date : July 17, 2022
Date received : July 27, 2022

Keywords:
Attendance; COBIT 4.1; PT DSN

ABSTRACT

The Fingerprint attendance system helps companies control employee working hours more efficiently and improve operational work activities using computerized tools, which can record the attendance list of each company employee. They were conducted following the COBIT Framework 4.1 standards for IT governance. It is necessary to conduct an audit to evaluate the information system's current governance. The research focuses on the sub-domains of AI4, DS1, DS4, DS5, DS10, and ME2. This research aims to analyze Fingerprint attendance system using COBIT Framework 4.1 standards for IT governance at PT DSN. This research uses observation, interview and literature techniques. The data analysis technique used is Maturity level. From the results of the study, it was found that DS5 was at the level of 3.02; DS4 and DS10 were at level 3 (Defined Process); DS1 was at the level of 2.8; AI4 was at level 2.7 (Repeatable but Intuitive); while ME2 is at the level of 1.7 (Initial/ad Hoc). The highest score is on DS5 (Ensure Systems Security) with a value of 3.02, and the lowest is on ME2 (Monitor and Evaluate Internal Control) with a value of 1.7.

INTRODUCTION

The development of increasingly advanced technology guides the business world to compete effectively and efficiently (Candrawati, 2013). Aid for ICT in local governments is highlighted above other aid provided for other activities due to the government's basic dependence on ICT in the present day (Lozoya-Arandia & Franco-Rebored, 2012). PT DNS is one of the companies engaged in bag convection (Candra, Atastina, & Firdaus, 2015). Attendance information system fingerprint at the company. It is necessary to evaluate the system and processes to ensure the company's attendance information system provides convenience in its business processes. Procedures applied to the company (Andry, 2017). The IS/IT audit within the COBIT framework can provide input on improving system management in the future (Kristianto, n.d.; Pradini & Andry, 2018).

Information System Audit is based on the framework COBIT 4.1 Control Objective for Information and Related Technology (COBIT) is a framework and supporting toolset that can

How To Cite: Salsabilla, A. T., et al. (2022). Audit of Attendance Information System with Fingerprint Using Cobit 4.1 Framework at PT DSN. *Journal of Social Science. 3*(4). https://doi.org/10.46799/jss.v3i4.379
E-Issn: 2721-5202
Published By: Ridwan Institut

help managers in companies bridge the gap between the goals of the company's needs for control, business risks faced and every technical problem, and communicate the level of control to stakeholders (Rozas & Effendy, 2012). COBIT has 4 main domains: Planning and Organization (PO), Acquisition and Implementation (AI), Delivery and Support (DS) and Monitoring and Evaluation (ME), which have processes (sub-domains) (Andry, 2016). The number of processes from each sub-domain is 34 processes.

The process of collecting and evaluating evidence determines whether the computerized application system establishes and implements the system in internal control adequately, ensures data integrity, and operates computer-based information systems effectively (Sukmajaya & Andry, 2017). Attendance The attendance system is a system that records the attendance list and the identity of each employee or member of the agency in a company (Iksan, Lumenta, & Sinsuw, 2016). A fingerprint is a tool used to facilitate a process of attendance activities in the company. In addition, it also serves to avoid manipulation of attendance data, which is very easy to do if the attendance process is done manually.

COBIT is a framework and supporting toolset that helps managers to control, technical issues and business risks as well as communicate with stakeholders regarding the level of control (Pradini & Andry, 2018). Companies can use the complete COBIT framework or employ specialized controls. COBIT provides guidelines on how to develop software and how to handle security with a consumer (Wolden, Valverde, & Talla, 2015). It is a basic framework method for creating IT according to the wishes of the organization. This method is a framework consisting of a domain and a process for managing activities and logical structures (Yulianti & Patria, 2011). The COBIT framework can be seen in Figure 1.

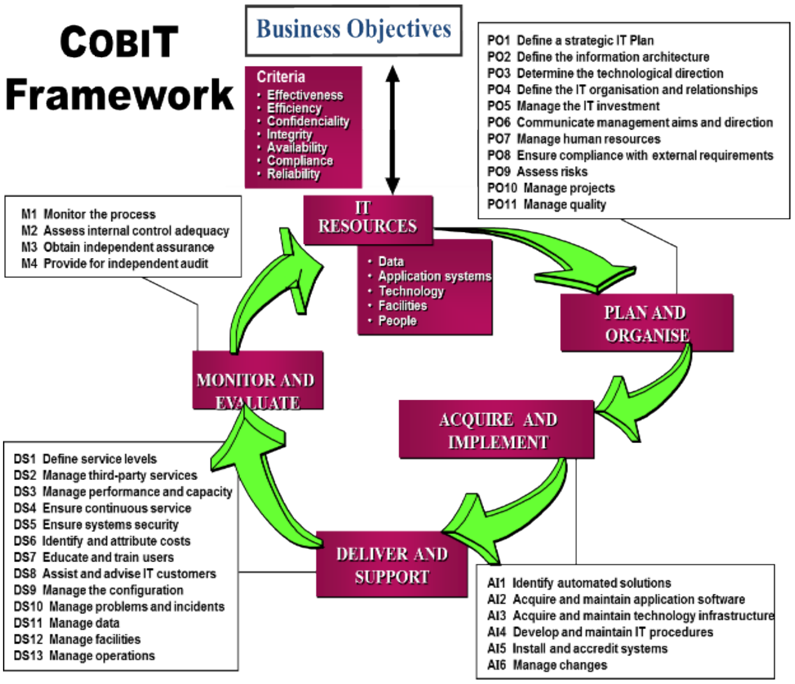
COBIT
Framework
Business Objectives
Criteria
• Effectiveness
• Efficiency
• Confidenciality
• Integrity
• Availability
• Compliance
• Reliability
PO1 Define a strategic IT Plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT organisation and relationships
PO5 Manage the IT investment
PO6 Communicate management aims and direction
PO7 Manage human resources
PO8 Ensure compliance with external requirements
PO9 Assess risks
PO10 Manage projects
PO11 Manage quality
M1 Monitor the process
M2 Assess internal control adequacy
M3 Obtain independent assurance
M4 Provide for independent audit
IT RESOURCES
• Data
• Application systems
• Technology
• Facilities
• People
PLAN AND ORGANISE
MONITOR AND EVALUATE
ACQUIRE AND IMPLEMENT
DELIVER AND SUPPORT
DS1 Define service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and attribute costs
DS7 Educate and train users
DS8 Assist and advise IT customers
DS9 Manage the configuration
DS10 Manage problems and incidents
DS11 Manage data
DS12 Manage facilities
DS13 Manage operations
AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire and maintain technology infrastructure
AI4 Develop and maintain IT procedures
AI5 Install and accredit systems
AI6 Manage changes

Figure 1. COBIT framework
(Sukmajaya & Andry, 2017)

In measuring the level of maturity for the management level and managers, it must be arranged because to know the management and processes of IT in the organization so that it can be known at which level of management. The maturity models used are:

1) 0 - Non-existent - There is no visible process at all.
2) 1 - Initial/Ad Hoc - There is evidence the company is aware that there is a problem and should be reviewed, but there is no standardization yet.
3) 2 - Repeatable but Intuitive - The process is developed at the stage where similar procedures are followed by various people performing the task.
4) 3 - Defined Process - Procedures have been standardized and documented, as well as communication through training.
5) 4 - Managed and quantifiable - Management monitors and measures the conformity of procedures and takes action where processes do not appear to be running effectively.
6) 5 - Optimized - The process is designed to a good level of implementation, based on the results of continuous development and maturity modeling with other companies.

Therefore, this study uses several domains: AI, DS, and ME. Especially in its sub-domains such as AI4, DS1, DS4, DS5, DS10, and ME2. This study chose this subdomain because it relates to the things that will be assessed, starting from employees, equipment, physical security, and regulations in the company, as well as finding gaps or gaps that determine the level of maturity in the application of attendance information systems and finding out alignment (Fitrianah & Sucahyo, 2008). The work process of the company's attendance procedures (Juliandarini & Handayaningsih, 2013).

This research on evaluating fingerprint attendance information systems with the COBIT framework is to measure the level of accuracy and effectiveness, whether it has been running according to PT DNS's target needs, and has a positive impact on employee performance. The value of the results of this study is expected to be useful as a decision-making material for the company's operational interests

METHOD

This study's scope of research is limited to auditing attendance information systems at PT. Sinar Pratama Agung and Identification of Attendance Information System Process.

Table 1
Coverage of IT Domains audited

Sub Domain	Descriptions
AI4	Enable Operations and Use
DS1	Define and Manage Service Levels
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS10	Manage Problems
ME2	Monitor and Evaluate Internal Control

The research methodology and stages in obtaining data from sources, starting from the initial survey and interviews, are shown in Figure 1. At this stage, the information technology process is determined by the COBIT standard, which is processed according to the case study. The scope of the IT domain audited in the attendance information system is shown in Figure 2.

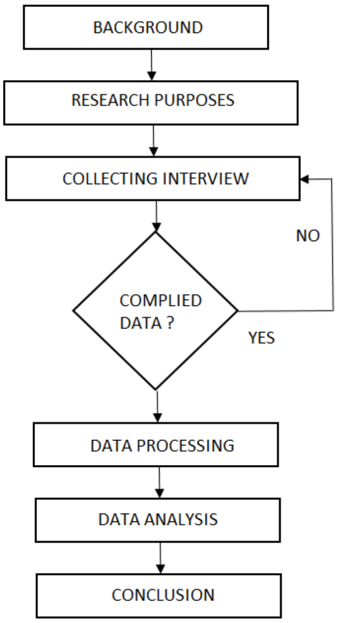

Figure 2. Research flow chart

The research procedure is an activity carried out in research. The stages and research procedures are as follows:

(1) Planning

Planning is the initial stage in the research procedures carried out. The design phase includes several main activities, namely determining the scope and objectives of the audit, organizing the audit team, understanding the client's business operations, reviewing the results of previous audits, and preparing an audit program. Because at this stage, the scope is determined*,* an object to be audited, evaluation standards from the audit results and communication to the person concerned about the organization/company to be audited by analyzing the vision, mission, objectives and objectives of the object, and policies. Policies are related to investigative processing.

(2) Field Inspection

At this stage, the auditor aims to obtain information by collecting data from related parties using several methods such as; an interview and a survey directly to the place where the research was conducted. The data obtained will be instrumental in helping the auditor analyze an organization/company being audited.

(3) Reporting

Reporting on a problem, it will be apparent where the error is. After that, the researcher will analyze and conclude the results. The researcher gives a report on the audit results in recommending corrective actions and the authority for improvement to the management object of research. Can this research be applied directly or only as a reference for future improvements.

(4) Follow-Up

By reporting a problem, it will be apparent where the error is. After that, the researcher will analyze and conclude the results. The researcher gives a report on the audit results in recommending corrective actions and the authority for improvement to the management object of research, can this research be applied directly or only as a reference for future improvements.

RESULTS AND DISCUSSION

In this section, Audit results and discussion will be explained the attendance information system with the COBIT framework at PT. DSN. Here, analyse the IT department's environment, including employees, equipment, physical security and regulations.

A. AI4 Enable Operation and Use

The process requires documentation and standard manuals used by users and IT. Training ensures that applications and infrastructure are used and run correctly (Tjee & Christianto, 2018).

1. **AI4.1 Planning for Operational Solutions**

   Operation solution planning by developing plans, identifying and documenting the technical aspects of operations and deployment so that everyone who operates and uses maintains automated solutions can carry out their responsibilities.

2. **AI4.2 Knowledge Transfer to Business Management**

   Knowledge transfer business management transferring business management enables individuals to take ownership of systems and data, responsibility for service provision and quality, internal control, and application administration.

3. **AI4. Knowledge Transfer to Operations and Support Staff Transfer**

   Operational knowledge and support staff transfer of knowledge and skills enables operations and technical support staff to effectively and efficiently support and maintain systems and associated infrastructure. The results of the AI4 Enable operation and use show that the maturity level of each process in its stages and processes can be seen in Table 2 of the Maturity AI4 Enable Operation and Use.

Table 2
Results Maturity AI4 enable operation and use

AI4 Enable operation and use		Maturity Level
AI4.1	Planning for Operational Solutions	3
AI4.2	Knowledge Transfer to Business Management	2
AI4.3	Knowledge Transfer to Operations and Support Staff	3
AI4	**Average**	**2,7**

B. DS1 Define and Manage Service Levels

Effective communication between IT management and business customers regarding required services. This process includes monitoring and regularly reporting to *stakeholders* for service level compliance. Processes enable alignment between IT services and related business requirements (Tjee & Christianto, 2018).

1. **DS1.1 Service Level Management Framework**

   Define a framework that provides service-level management processes between customers and service providers. The framework maintains alignment between business needs and priorities and facilitates common understanding between customers and providers. The framework includes processes for creating service requirements, service definitions, SLAs, OLAs and funding sources.

2. **DS1.2 Service Level Agreements**

   Define and agree on SLAs for all critical IT services based on customer requirements and IT capabilities, such as customer commitments, support service requirements, funding and commercial arrangements, etc.

3. **DS1.3 Operating Level Agreements**

   Establish an OLA that describes how the service will be delivered technically to support the SLA optimally.

4. **DS1.4 Monitoring and Reporting of Service Level Achievements**

   Monitor specific service level performance criteria and report achievements. The results statistics are analyzed to identify strengths and weaknesses to improve services.

5. **DS1.5 Review of Service Level Agreements and Contracts**

   Audit analysis Define and manage service levels. Regularly review SLAs and foundation contracts (UCs) with internal and external service providers ensuring they are practical and up to date and changes in requirements have been taken into account. The maturity level of each process in the stages and processes can be seen in Table 3.

Table 3
Results of Maturity DS1 Define And Manage S

	DS1 Define And Manage Service Levels	**Maturity Level**
DS1.1	Service Level Management Framework	2
DS1.2	Service Level Agreements	
DS1.3	Operating Level Agreements	3
DS1.4	Monitoring and Reporting of Service Level Achievements	3
DS1.5	Review of Service Level Agreements and Contracts	3
DS	**Average**	**2,8**

C. DS4 Ensure Continuous Service

Providing continuous IT services requires developing, maintaining and testing an IT continuity plan, utilizing offsite backup and providing periodic continuity plan training (Tjee & Christianto, 2018).

1. **DS4.1 IT Continuity Framework**

   The framework discusses the organizational structure of continuity management, covering the roles, duties and responsibilities of internal and external service providers, management and customers, planning processes that create rules and document structures, and testing and implementing IT disaster recovery and contingency plans.

2. **DS4.2 IT Continuity Plans**

   Plans are based on understanding the risks of potential business impact and address requirements for resilience, alternative processing and recovery capabilities of all critical IT services.

3. **DS4.3 Critical IT Resources**

   Focus on the items specified as most critical in the IT continuity plan for building resilience and setting priorities in recovery situations.

4. **DS4.4 Testing of the IT Continuity Plan**

   Testing the IT continuity plan regularly ensures IT systems can recover effectively, address deficiencies and keep the plan relevant.

5. **DS4.5 IT Continuity Plan Training**

   Provide all relevant parties regular training sessions on procedures and their roles and responsibilities in an incident or disaster.

6. **DS4.6 Distribution of the IT Continuity Plan**

   Determine the existence of the definition and management of the distribution strategy, ensuring the plan is distributed correctly and safely and is available to interested parties when and where needed.

7. **DS4.7 IT Services Recovery and Resumption**

   Activation of backup sites, alternative processes, customer and stakeholder, and forwarding procedures.

8. **DS4.8 Post-resumption Review**

   Determine whether IT management has established procedures to assess the adequacy of the plan for the successful continuation of the IT function after a disaster, and update the plan accordingly. Audit analysis Ensure continuous service, the maturity level of each process in stages and processes can be seen in Table 4 of the DS4 Ensure continuous service.

Table 4
Maturity DS4 Ensure Continuous Service

DS4 Ensure Continuous Service		Maturity Level
DS4.1	IT Continuity Framework	2
DS4.2	IT Continuity Plans	3
DS4.3	Critical IT Resources	3
DS4.4	Testing of the IT Continuity Plan	3
DS4.5	IT Continuity Plan Training	2,5
DS4.6	Distribution of the IT Continuity Plan	3
DS4.7	IT Services Recovery and Resumption	2
DS4.8	Post-resumption Review	3
DS4	**Average**	**3**

D. DS5.1 Ensure Systems Security

Effective security management protects all IT assets minimizing the business impact of security vulnerabilities and incidents. The process includes establishing and maintaining IT security roles and responsibilities, policies, standards, and procedures. Security management includes monitoring, periodic testing, and implementing corrective actions to identify security vulnerabilities or incidents.

1. **DS5.2 Identity Management**

   Ensure that all users (internal, external and temporary) and activities in IT systems (business applications, IT environment, system operations, development and maintenance) are uniquely identifiable. Confirm the user has access rights to the system and data by defining and documenting business needs and work requirements attached to the user identity.

2. **DS5.3 Security Testing, Surveillance and Monitoring**

   Test and monitor IT security implementation in a proactive manner. The logging and monitoring functions enable early prevention and timely detection and reporting of unusual and abnormal activities that may need to be addressed. IT Security is re-accredited promptly, ensuring the company's approved information security base is maintained.

3. **DS5.4 Protection of Security Technology**

   Create security-related technologies that are resistant to intrusion.

4. **DS5.5 Cryptographic Key Management**

   Establish policies and procedures governing the generation, alteration, revocation, destruction, distribution, certification, retention, entry, use and archiving of cryptographic keys ensuring protection against essential modification and unauthorized disclosure.

5. **DS5.6 Network Security**

   Uses security techniques and related management procedures (e.g., firewalls, security tools, network segmentation, intrusion detection) to authorize access and control the flow of information to and from the network.

6. **DS5.7 Exchange of Sensitive Data**

   Exchange sensitive transaction data via trusted or intermediate channels with controls providing content authenticity, proof of delivery, proof of acceptance and no rejection. Audit analysis Ensure Systems Security, the maturity level of each process in the stages and processes can be seen in Table 5.

Table 5
Results of Maturity DS5 Ensure Systems security

DS5 Ensure Systems Security		**Maturity Level**
DS5.1	Management of IT Security	3
DS5.2	Identify Management	3
DS5.3	Security Testing, Surveillance and Monitoring	2
DS5.4	Protection of Security Technology	3
DS5.5	Cryptographic Key Management	3
DS5.6	Network Security	4
DS5.7	Exchange of Sensitive Data	3
DS5	**Average**	**3,02**

E. DS10 Manage Problem

Effective data management requires identifying data requirements. The data management process includes establishing procedures for managing the media library, backup and recovery data, and proper media disposal. Effective data management helps ensure business data quality, timeliness and availability.

1. **DS10.1 Identification and Classification of Problems**

   Implement a process for reporting and classifying problems identified as part of incident management. These steps involved in problem classification are similar to the steps in incident classification. These steps determine the category, impact, urgency, and priority. Categorize problems appropriately into related groups or domains (e.g. hardware, software). These groups are tailored to the organizational responsibilities of the user and consumer base. They should be the basis of problem allocation to support staff.

2. **DS10.2 Problem Tracking and Resolution**

   Ensure the problem management system provides an audit trail to facilitate tracking, analysis and determining the root cause of all reported problems regarding all related configuration objects, incidents and unresolved problems, errors suspected and known trends of the problem. Problem management must monitor the ongoing impact of errors known if the impact is severe. Problem management should escalate the problem, perhaps involving senior management to increase the report's priority or implement significant changes as needed. Monitor progress of problem resolution according to SLA.

3. **DS10.3 Problem Closure**

   Create a procedure for resolving problem reports that are executed when confirmation of an error is resolved or after agreement with the business on alternative paths to deal with the problem.

4. **DS10.4 Integration of Configuration, Incident and Problem Management**

   Integrating configuration, incident and problem management processes ensures effective management of problems and facilitates development. Audit analysis Manage Problems the maturity level of each process in the stages and processes can be seen in Table 6 of the Maturity DS10 Manage Problems.

Table 6
Results of Maturity DS10 Manage Problems

DS10 Manage Problem		Maturity Level
DS10.1	Identification and Classification of Problems	3
DS10.2	Problem Tracking and Resolutions	3
DS10.3	Problem Closure	3
DS10.4	Integration of Configuration, Incident and Problem Management	3
DS10	**Average**	**3**

F. ME2 Monitor and Evaluate Internal Control

Building an effective internal control program for IT requires a well-defined monitoring process. The process includes monitoring and reporting exception controls and collecting internal and third-party assessments. The critical advantage of monitoring internal controls is to ensure effective and efficient operation and compliance with applicable laws and regulations.

1. **ME2.1 Supervisory Review**

   Monitor and evaluate the efficiency and effectiveness of internal IT managerial review controls.

2. **ME2.2 Control Exceptions**

   Underlying cause root. Improved exception control and reporting appropriately to stakeholders. Institute corrective action is required.

3. **ME2.3 Control Self-assessment**

   A continuous self-assessment program will evaluate the completeness and effectiveness of management control over IT processes, policies and contracts.

4. **ME2.4 Internal Control at Third Parties**

   Assess the status of the external service provider's internal controls. Ensure external service providers comply with legal and regulatory requirements and contractual obligations.

5. **ME2.5 Remedial Actions**

   Identify, track and implement corrective actions arising from control assessment and reporting. Audit analysis Monitor and Evaluate Internal Control the maturity level of each process in the stages and processes can be seen in Table 7.

Table 7
ME2 Monitor and Evaluate Internal Control Maturity Results and Evaluate ME2 Monitor

ME2 Monitor and Evaluate Internal Control		Maturity Level
ME2.1	Supervisory Review	2
ME2.2	Control Exceptions	3
ME2.3	Control Self-assessment	2
ME2.4	Assurance of Internal Control	0
ME2.5	Remedial Actions	2
ME2	**Average**	**1,70**

The attendance information system audit results above show the sub-domain average maturity levels in Table 8. The overall desired maturity (to-be) is at level 4, namely Managed and measurable, compared to the current maturity (as-is). The data in Table 8 shows the average maturity levels made using a spider, shown in Figure 3.

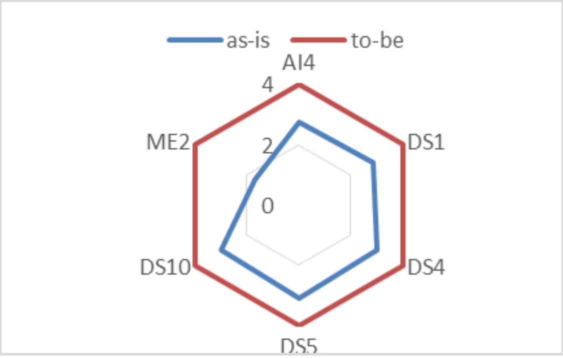

Figure 3. Spider Maturity Level diagram as-is vs to-be

Table 8
Average Maturity Level

Proses TI	Descriptions	Maturity Level
AI4	Enable operation and use	2,7
DS1	Define And Manage Service Levels	2,8
DS4	Ensure Continuous Service	3
DS5	Ensure Systems Security	3,02
DS10	Manage Problem	3
ME2	Monitor and Evaluate Internal Control	1,7

CONCLUSION

The conclusions that can be drawn from the research that has been done are as follows: (1) The existence of information system governance at PT. DSN is well-defined and formal. There are standard procedures and guidelines from the management, and (2) based on the measurement results using the maturity level, it is known that DS5 is at level 3.02 and DS4 and DS10 are at level 3 (Defined Process), while DS1 is at level 2.8 and AI4 at level 2.7 (Repeatable but Intuitive), while ME2 is at level 1.7 (Initial/ad Hoc). The highest score is on DS5 (Ensure Systems Security) with a value of 3.02, and the lowest is on ME2 (Monitor and

Evaluate Internal Control) with a value of 1.7. With that, it is known that the Attendance Information System Governance at PT. DSN is level at level 3.

REFERENCES

Andry, F. J. (2016). Audit Tata Kelola TI Di Perusahaan (Studi Kasus XYZ Cargo). *Seminar Nasional Teknologi Informasi*, 1–9. Google Scholar

Andry, J. F. (2017). Audit Sistem Informasi Absensi Pada Pt. Bank Central Asia Tbk Menggunakan Cobit 4.1. *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(2). Google Scholar

Candra, R. K., Atastina, I., & Firdaus, Y. (2015). Audit teknologi informasi menggunakan framework COBIT 5 pada domain DSS (Deliver, Service, and Support)(Studi kasus: IGRACIAS Telkom University). *EProceedings of Engineering*, *2*(1). Google Scholar

Candrawati, P. (2013). Sistem Informasi Absensi Karyawan Pada PT Harja Gunatama Lestari Bandung. *Jurnal Computech & Bisnis*, *7*(2), 96–105. Google Scholar

Fitrianah, D., & Sucahyo, Y. G. (2008). Audit Sistem Informasi/Teknologi Informasi dengan kerangka kerja COBIT untuk evaluasi manajemen teknologi informasi di Universitas XYZ. *Jurnal Sistem Informasi*, *4*(1), 37–46. Google Scholar

Iksan, T. S., Lumenta, A. S. M., & Sinsuw, A. A. E. (2016). Pembuatan Aplikasi Administrasi Kantor Jurusan Teknik Elektro Fakultas Teknik Unsrat. *Jurnal Teknik Elektro Dan Komputer*, *5*(2), 59–66. Google Scholar

Juliandarini, J., & Handayaningsih, S. (2013). *Audit Sistem Informasi Pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0*. Universitas Ahmad Dahlan. Google Scholar

Kristianto, M. (n.d.). *Perancangan Pedoman Audit Sistem Informasi Pada Industri Perhotelan dengan Studi Kasus Hotel Bintang 4 Berbasis Framework COBIT 4.1 menggunakan Domain Delivery and Support*.

Lozoya-Arandia, J., & Franco-Rebored, C. (2012). Insights on the definition of an agenda for ICT development in municipal governments: A reference model. *Procedia Technology*, *3*, 282–291. Scopus

Pradini, T., & Andry, J. F. (2018). Audit Sistem Informasi Front Office Pada World Hotel Menggunakan Kerangka Kerja COBIT 4.1. *Ikraith-Informatika*, *2*(1), 18–25. Google Scholar

Rozas, I. S., & Effendy, D. A. (2012). Mengukur efektifitas hasil audit teknologi informasi cobit 4.1 berdasarkan perspektif End User. *JURANAL LINK*, *17*. Google Scholar

Sukmajaya, I. B., & Andry, J. F. (2017). Audit Sistem Informasi Pada Aplikasi Accurate Menggunakan Model Cobit Framework 4.1 (Studi Kasus: Pt. Setia Jaya Teknologi). *Prosiding Seminar Nasional Teknoka*, *2*, I42–I51. Google Scholar

Tjee, C., & Christianto, K. (2018). Evaluating of IT Services on Accurate Application Using COBIT 5 (Case Study: PT. SS Dinamika). *Jurnal Teknik Informatika Dan Sistem Informasi*, *4*(2), 270–280. Google Scholar

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, *48*(3), 1846–1852. Scopus

Yulianti, D. T., & Patria, M. C. (2011). Audit Sistem Informasi Sumber Daya Manusia Pada PT X Menggunakan Cobit Framework 4.1. *Jurnal Sistem Informasi*, *6*(1), 15–33. Google Scholar