p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 5, No. 4 April 2024 http://jist.publikasiindonesia.id/

Implementation Planning Information Technology Service Management (ITSM) Iso 20000-Based in Guarantee Companies

Ahmad Kahfi[1*], Nilo Legowo[2]
Universitas Bina Nusantara Jakarta, Indonesia
Email: ahmad.kahfi@binus.ac.id[1*], nlegowo@binus.edu[2]

*Correspondence

Keywords:
ITSM, ISO 20000, Service level agreement (SLA), Guarantee Company, helpdesk.

ABSTRACT

The helpdesk work unit was formed as a basic implementation of Information Technology Service Management (ITSM) implementation in the Company. In order to be able to measure the implementation of ITSM in the company, standardization of service management is needed; currently, the standard used as a reference and widely used is ISO 20000. ISO 20000 is a reference or best practice used in the implementation of business process management, which is expected to be able to respond to globalization developments where the ultimate goal to be achieved is to improve the quality and service in the Company. Currently, the constraints and problems faced by the Guarantee Company when ITSM has not been implemented include poor IT management, reduced levels of trust from stakeholders, weak control functions so that many risks occur and service level agreements (SLA) become unclear or do not have indicators in providing services.

Introduction

The Company has formed an IT Helpdesk work unit to provide information or resolve service requests and IT problems reported by all existing work units. The helpdesk work unit was formed as a basic implementation of Information Technology Service Management (ITSM) implementation in the Company (Ramadhan, 2019). Standardization of service management is needed to measure the implementation of ITSM in the company. Currently, the standardization used as a reference and widely used is ISO 20000. By using ISO 20000 as a reference or as best practice in implementing business processes, management is expected to be able to respond to developments in globalization where the final goal to be achieved is to improve the quality and service in the Company (Amir, 2018).

In implementing and managing IT services for quality and meeting business needs, ITSM is the right step as a solution. IT service providers perform ITSM processes through the right mix of people, processes, and information technology (Romadini, Santoso, &

Santosa, 2018). This refers to the processes, policies, and procedures that help organizations plan, manage, and implement IT services. ITSM's primary goal is to align IT with business needs; this is necessary to change IT, which has long been considered a firefighting team, to become a reliable service provider for interns (Priyadi, Saedudin, & Fauzi, 2019). Currently, ITSM not only focuses on IT usage or services but also focuses on efforts to provide a framework for structuring IT-related activities and interactions between IT technical personnel and IT users. There are many standard IT management frameworks from various aspects of review. Service management is one of the standard IT management frameworks (Priyohutomo & Sitokdana, 2020). IT governance framework standards include the Infrastructure Technology Information Library (ITIL) and ISO/IEC 20000. IT service management includes ITIL and ISO 20000 based on the framework standards mentioned (Setiawan & Sfenrianto, 2023). ITIL is a set of concepts and techniques managing IT infrastructure, development, and operations and is often used as a reference in implementing ITSM in an organization in describing details on processes, procedures, tasks, and checklists to build integration between IT and organizational strategy in providing value and maintaining a minimum level of (Kusbandono, Ariyadi, & Lestariningsih, 2019).

Guarantee Companies face problems when ITSM has not been implemented, including lack of proper IT management, lack of trust from stakeholders, lack of control so that many risks occur, and the service level agreement (SLA) is unclear or cannot be an indicator in providing services (Utami, 2010). As a result of the lack of clarity on the SLA, incident management is critical in solving problems in the Guarantee Company because incident management will be related to several problems, including change management, service level agreement, and problem management (Hariyanti, Sihombing, & Wirapraja, 2018).

Theoretical Basis

ITSM is implementing and managing IT services to ensure quality and meet business needs. IT Service Management is performed by IT service providers through the right mix of people, processes, and information technology (Pratama & Sutabri, 2023). ITSM as a management solution is not only related to the availability of information technology (IT) infrastructure but also how this infrastructure can be used to improve the quality of IT services in the corporate environment so that it becomes more efficient and effective, which results in the ability to optimize service to customers. While saving costs.

An application is a software (software) or computer program operating on a particular system that is created and developed to perform specific commands. The term application itself is taken from the English word "application," which can be interpreted as an application or use. An application is software or software developed to perform specific tasks.

The application can be concluded as a ready-to-use program that helps achieve user goals. A ready-to-use program application that can be used to run commands from the application user to get more accurate results by the purpose of making the application, the application has a meaning, namely solving problems using one of the application data processing techniques that usually races on a desired or expected computation as well as expected data processing.

Quoted from (ISO IEC 20000-1, 2019) The ISO 20000 standard is an information technology (IT) management certification developed to replace the British Standard (BS) 15000 certification established by British Standards International (BSI). Developed as a joint project by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), this standard is also known as IEC 20000.

Based on (ISO IEC 20000-1, 2019), ISO 20000 defines the requirements for establishing, implementing, maintaining, and continuously improving a service management system (EMS). EMS supports the management of the service life cycle, including planning, design, transition, delivery, and improvement of services that meet agreed-upon requirements and benefit customers, users, and the organization providing the service. The adoption of an EMS is a strategic decision for an organization. It is influenced by the goals of that organization, regulatory agencies, and other parties involved in the service life cycle and the need for effective and elastic services. Implementing and operating an EMS provides ongoing visibility, service control, and continuous improvement, leading to higher effectiveness and efficiency. Service management improvements apply to EMS and services.

Key Issues And The Challenges

One of the problems in Service Management is the limited documentation of technical problems. The company's data processing techniques are still done manually by recording tickets, processing service requests, and reporting incidents and problems, which are still processed manually with the help of spreadsheets. Apart from that, in the Service Management system for service requests, incidents, and problem reporting by users to the Helpdesk work unit, namely using the WhatsApp application, which makes the Helpdesk's services less effective; this problem makes reports complaints by users often become recurring reports.

The Helpdesk reflects the IT Operations Division's services, which act as a single point of contact in interactions with users and related departments within the scope of information technology services. The Helpdesk manages incidents and issues from users through coordination with other divisions in the company. It represents these work functions into business processes, not infrequently due to frequent user interactions. Helpdesk agents can solve problems whose answers are unknown by the division other.

Research Methods

This research seeks how to apply the ITSM concept to the ISO 20000 concept, which is adapted to the conditions of the Company in terms of stages and procedures for the tools to be used. This is to find out the condition of the existing IT service management process so that the resulting recommendations can be suitable on target. This research model is proven empirically with the following stages:

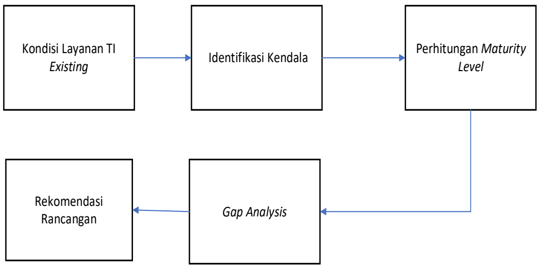


Figure 1. Thinking Framework

Recommendations for implementing ITSM are obtained from an analysis of the existing condition gap with ISO 20000 standardization and the existing conditions in the company. Based on this description of the condition of the Guarantee Company is based on direct observation by conducting interviews based on questionnaires and complementary documents obtained from the Company, both related to policies or procedures and tools used to provide IT services to all users in the Company.

In this research step, the author will explain in detail the stages that will be carried out to identify and solve problems in the research object being carried out, namely:

1. Existing Condition of IT Services
2. Identify Constraints

The method collecting data from this study uses several methods, namely interviews where the author conducts a series of interviews or questions and answers to several work units where the work unit is a user of IT services; this is to find out the extent of the obstacles in the IT sector that are reported to get appropriate services. With observation, the author makes direct observations at the Guarantee Company, especially in the IT Operations Division, to find out how to run IT services directly. Finally, the questionnaire is a technique used by the author to calculate the current condition of IT services.

The ISO 20000 standard is aligned with the ITSM/ITIL framework based on BSI, ITSMF, and the Office of Government Commerce (OGC), and the two standards have different objectives. ITIL provides a best practice guide on how to implement ITSM. Meanwhile, ISO/IEC 20000 defines a series of requirements for ITSM, and based on these requirements, service certification activities can be carried out against existing standards. The relationship between ISO 20000 and the ITIL standard can be seen in the image below:

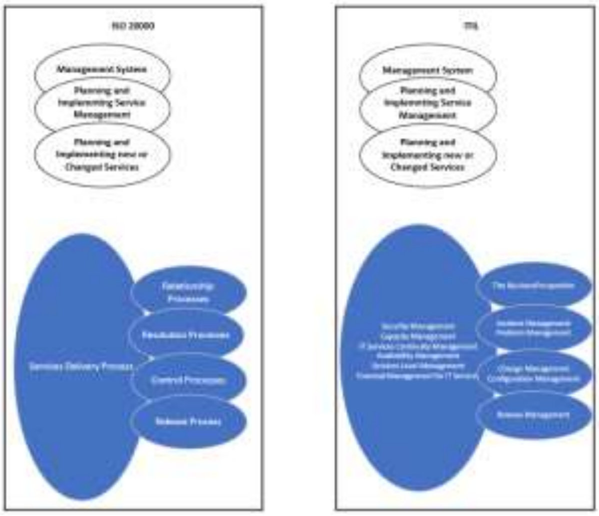


Figure 2. Relationship between ISO 20000 and ITIL

Results and Discussion

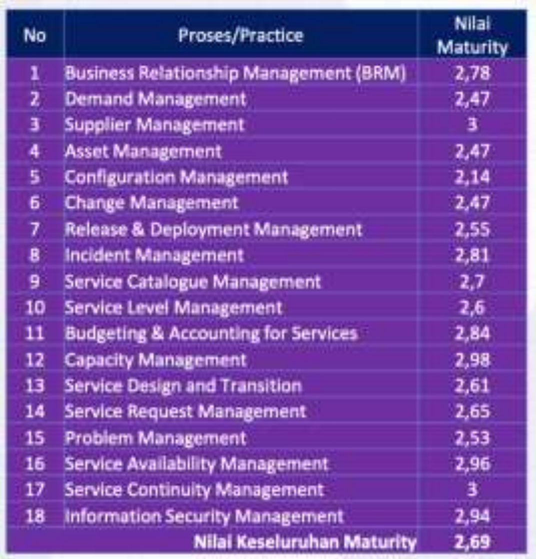
Guarantee Company

Departing from the actual conditions of the development of cooperatives, which were still lagging compared to the other two economic actors (BUMN and Private), the Government established the Cooperative Credit Guarantee Institution (LJKK) in 1970, which in its development was changed to the Public Corporation for Cooperative Financial Development (Perum PKK) through Regulation Government Number 51 dated December 23, 1981, which was later refined by PP No. 27 dated May 31, 1985.

Through Government Regulation No. 11 of 2022, the legal entity of the Guarantee Company, which was initially a Public Company, was officially changed to a Limited Liability Company as a Guarantor running a B2B (Business to Business) business process providing guarantees to the Guarantee Recipient/Guarantee for all financing made to the Guaranteed party.

Maturity Level Measurement

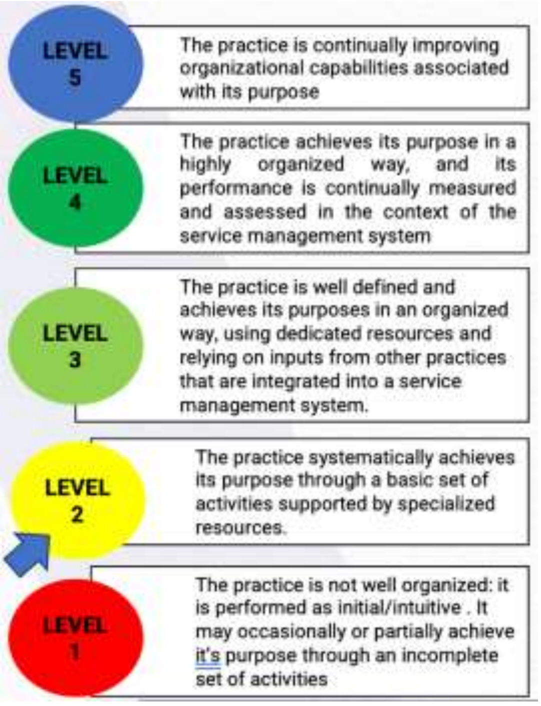
Maturity level measurement uses the ITIL Self Assessment Study, which is the basis for selecting access management as part of the research conducted by researchers. This maturity level measurement uses the interview method with the relevant work units in assessing the current condition of the IT Service Management (ITSM) Maturity Level Assessment, which is carried out covering 18 processes which include processes in ITIL version 4 best practices as well as ISO/IEC standards 2000-1:2018. The results of the measurements can be seen in the following figure.



No	Proses/Practice	Nilai Maturity
1	Business Relationship Management (BRM)	2,78
2	Demand Management	2,47
3	Supplier Management	3
4	Asset Management	2,47
5	Configuration Management	2,14
6	Change Management	2,47
7	Release & Deployment Management	2,55
8	Incident Management	2,81
9	Service Catalogue Management	2,7
10	Service Level Management	2,6
11	Budgeting & Accounting for Services	2,84
12	Capacity Management	2,98
13	Service Design and Transition	2,61
14	Service Request Management	2,65
15	Problem Management	2,53
16	Service Availability Management	2,96
17	Service Continuity Management	3
18	Information Security Management	2,94
	Nilai Keseluruhan Maturity	2,69

Figure 4. ITSM Maturity Level (IT Operations) Year 2023

ITSM implementation in Guarantee Companies is already at level 2 with a maturity value 2.69. The highest score is in the Supplier Management and service continuity management processes, with a maturity value of 3 each, while the lowest score is in the Configuration Management process, with a maturity value of 2.14. The things that become gaps for configuration management are that the process has started but is done manually, there is a lack of personnel for configuration management, where the role is still concurrent with other processes, there are no specific tools that support the Configuration Management process, there is no relationship between configurations Item, and - Configuration Item. or Configuration Management Database audit has not been performed.



The practice is continually improving organizational capabilities associated with its purpose

The practice achieves its purpose in a highly organized way, and its performance is continually measured and assessed in the context of the service management system

The practice is well defined and achieves its purposes in an organized way, using dedicated resources and relying on inputs from other practices that are integrated into a service management system.

The practice systematically achieves its purpose through a basic set of activities supported by specialized resources.

The practice is not well organized: it is performed as initial/intuitive . It may occasionally or partially achieve it's purpose through an incomplete set of activities

Figure 5. Level And Descriptions

Needs Analysis

Based on the results of the analysis obtained from the researcher, the researcher recommends that the Central Information Systems Department complete several points that researchers consider necessary, including IT Policy, Verification of data confidentiality, and Control of access rights.

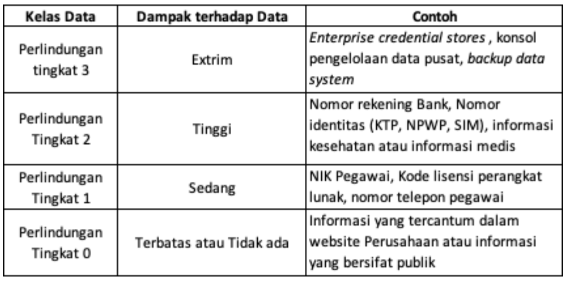
Information Technology Policy

the first is the use of the accepted policy. Namely, this Policy determines the accepted policy for all technological resources owned by the Company. The second is the Access Policy, which establishes access guidelines for all the Company's technological resources. This policy aims to ensure that every employee in the company is provided with equal learning facilities and that all staff can adequately use the necessary technological tools to achieve common goals. The third is the access policy, which sets out the access guidelines for all technological resources owned by the Company. This policy aims to ensure that every Guarantee Company Employee is provided with equal facilities for learning and that all staff can adequately use the necessary technological equipment to achieve common goals.

The fourth is a backup policy where the IT Operations Division ensures procedures for storing essential data for each department or individual. The fifth is the electronic communication policy, where electronic communication is required to fulfill multiple roles and activities in the Company because various types of electronic communication will focus on those used by the Company. The sixth is a sensitive information policy in which the Company's main focus is information sensitivity. Because we are an educational entity, we deal with many different types of information, some for general purposes and some not. This policy is intended to help employees determine what information can be disclosed to non-staff and the relative sensitivity of information that should not be disclosed outside the Company without proper authorization.

Confidentiality Verification Data

Confidential data holds the most important values and carries excellent risks in an organization or specific individuals. Based on these details, it is necessary to verify the confidentiality of data, which relates to the confidentiality of said data. Confidential data addressed includes the entire organization and hard copies of organizational data. The purpose of verifying the confidentiality of data is necessary due to the challenge of maintaining personal or confidential data. In this case, the risks found are identity data theft, unauthorized or illegal changes to data, manipulation of financial data related to access to electronic information, and data confidentiality of the data collection process. Confidentiality verification can also be carried out by controlling access rights, where control is carried out by establishing official rules that allow users to remotely access and manipulate personal information, network applications, and other data from outside the Company.



Kelas Data	Dampak terhadap Data	Contoh
Perlindungan tingkat 3	Extrim	*Enterprise credential stores* , konsol pengelolaan data pusat, *backup data system*
Perlindungan Tingkat 2	Tinggi	Nomor rekening Bank, Nomor identitas (KTP, NPWP, SIM), informasi kesehatan atau informasi medis
Perlindungan Tingkat 1	Sedang	NIK Pegawai, Kode lisensi perangkat lunak, nomor telepon pegawai
Perlindungan Tingkat 0	Terbatas atau Tidak ada	Informasi yang tercantum dalam website Perusahaan atau informasi yang bersifat publik

Figure 6 Data Classification

Control of Access Rights

Access control is the first consideration when an Information Security System professional creates an information security program. The features and variations of access control mechanisms, both physically, technically, and administratively, will build a practical information security architecture to protect critical and sensitive information, which is an organizational asset. Privacy (individually) is one of the reasons for implementing access control in organizations. Technology has made the exchange of information more accessible and more widespread, so efforts to protect information are becoming more complex and challenging [17].

Control of access rights always leads to data confidentiality and several types of control of access rights in information security.

Prevention by physical control

In this case, several things need to be done. The first is to back up files/documentation to prevent an accident in the computer system, as essential files/documents remain. This backup document should be stored in a remote place with security measures equivalent to the active document. The second is fencing, which is limited so that only authorized persons can enter the system. In this case, CCTV and alarms are included in the fencing system and others. The third is an identification system, which recognizes that the person is a party granted specific access. The fourth is backup power, namely to ensure that there is no sudden power/electricity cut-off that will cause damage to the system. Back-up power is usually in spare batteries or a diesel generator. The most popular device is the UPS (uninterruptible power supply). The fifth is selecting a location where the factors are critical to avoid risks that may arise due to floods, fires, electromagnetic wave radiation, or others. Moreover the sixth is the fire department. Fire will damage the system. In addition to the fact that the system's location must be far from places that trigger fires, the material used should also be non-flammable.

Detection in physical control

Detection as physical control is a protection against violations that have already occurred. Like motion detectors, the computer server room area is generally not used for human activity traffic, so installing a motion detection device will be very useful in preventing intrusion. Smoke and fire detectors, if placed in the right place, will be handy as the fastest notification device in the event of a fire. CCTV (Closed-Circuit Television) monitors the area where the system is located/placed.

Technical control

This technical security includes using security guards, including computer hardware, operating systems, application software, communications, and other related equipment. Matters included in technical control include Prevention in technical control. Prevention is technically used to prevent unauthorized parties from accessing computer resources.

Administrative control

Administrative or security personnel consist of management restrictions, operational procedures, liability procedures, and additional administrative controls to protect computer resources adequately. Administrative controls include procedures to ensure that all personnel who gain access to computer resources obtain appropriate authorization and security clearance.

The IT Service Management (ITSM) Maturity Level Assessment measurement covers 18 processes, including the ITIL version 4 best practice process and the ISO/IEC 2000-1:2018 standard. With the following scope:

a) Business Relationship Management (BRM): Relationship management practices aim to build and maintain relationships between organizations and stakeholders at a strategic and technical level. This includes identification, analysis, monitoring, and continuous improvement of relationships with and between stakeholders.

b) Demand Management: The purpose of the business analysis practice is to analyze a business or some element of it, define its associated needs, and recommend solutions to address these needs and solve a business problem, which must facilitate value creation for stakeholders. Business analysis enables an organization to communicate its needs meaningfully, express the rationale for change, and design and describe solutions that enable value creation in alignment with the organization's objectives.

c) Supplier Management: Ensure ongoing engagement between customers and users through a feedback process and continuous service review.

d) Asset Management: IT Asset Management plays a role in the service value chain, with practices applied to design, transition, and value chain building activities.

e) Configuration Management: This contributes to collecting and managing information about various CIs, including hardware, software, networks, buildings, people, suppliers, and documentation.

f) Change Management: This is necessary because many changes start from the impact of new services or changes. Change control activities are central to the transition process.

g) Release & Deployment Management: Deployment management moves new and changed components to live environments, a vital element of value chain activity.

h) Incident Management: Incident Management contributes to the service value chain, which is applied mainly to engage, deliver, and support value chain activities. Except for plan, other activities may use information about incidents to help set priorities

i) Service Catalogue Management: Service catalog management contributes to the service value chain, with the practice being involved in all value chain activities

j) Service Level Management: Service level management contributes to the planning of the product and service portfolio and service offerings with information about the actual service performance and trends.
k) Budgeting & Accounting for Services: Service financial management supports decision-making regarding where to allocate financial resources best. It provides visibility into the budgeting, costing, and accounting activities related to the products and services.
l) Capacity Management: Capacity and performance management is essential for product and service design: it helps to ensure that new and changed services are designed for optimum performance, capacity, and scalability
m) Service Design and Transition: The purpose of service design is to design products and services that are easy to use, desirable, and the organization can deliver that.
n) Service Request Management: Service request management can provide a channel for improvement initiatives, compliments, and user complaints. It also contributes to improvement by providing trend, quality, and feedback information about the fulfillment of requests
o) Problem Management: Problem management makes a significant contribution by preventing incident repetition and supporting timely incident resolution
p) Service Availability Management, When planning and making improvements, availability management ensures that services are not degraded
q) Service Continuity Management, Service continuity management ensures that continuity plans, measures, and mechanisms are continually monitored and improved in line with changing internal and external circumstances
r) Information Security Management, The purpose of the information security management practice is to protect the information needed by the organization to conduct its business. This includes.

The highest score is in the Supplier Management and service continuity management processes, with a maturity value of 3 each, while the lowest score is in the Configuration Management process, with a maturity value of 2.14.

The recommendation from the above is to implement ITSM tools with modules that suit your needs. as well as the need for additional personnel who specifically carry out the management process of the modules to be used. Preparation of Operation Level Agreement that supports the Service Level Agreement It is necessary to review it so that it is known how far the effectiveness and efficiency of the process that has been carried out by the assessment and implementation of the Post Implementation Review for each service that has been implemented.

Conclusion

Based on the results of the analysis carried out on current conditions, the following conclusions can be drawn:

1) The current level of IT service governance maturity in the IT Operations Division of the guarantee company, measured based on the ITIL version 4 framework, is at level 2 – repeatable. This means that existing processes and activities already have a level of discipline and compliance.
2) Findings for the maturity level of each domain are different. The highest value is in the Supplier Management and Service Continuity Management processes, with a maturity value of 3 each. In contrast, the Configuration Management process occupies the lowest value with a maturity value of 2.14. The things that are gaps or gaps for configuration management are that the process has started to be carried out but is done manually, there is a lack of personnel for configuration management, where the role is still combined with other processes, there are no special tools that support the Configuration Management process, there is no relationship between Configuration Management. Items and - Configuration Item or Configuration Management Database audits have not been carried out.
3) The expected maturity target for the future is level 3 – defined where all existing processes and activities must be documented, standardized, and appropriately integrated.

Bibliography

Amir, Royhan. (2018). *Usulan tata kelola teknologi informasi (it Governance) menggunakan framework cobit 5 (studi kasus: Pt. bprs Al-salaam)*. Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah ….

Hariyanti, Novi Tri, Sihombing, Denny Jean Cross, & Wirapraja, Alexander. (2018). Pemanfaatan Proses Pada Kerangka Itilv3 Dalam Menyediakan Manajemen Layanan Teknologi Informasi. *Jurnal Eksekutif*, *15*(2), 388–403.

Kusbandono, Hendrik, Ariyadi, Dwiyono, & Lestariningsih, Tri. (2019). *Tata kelola teknologi informasi*. CV Nata Karya.

Pratama, Yoga, & Sutabri, Tata. (2023). Service Operation ITIL V3 Pada Analisis dan Evaluasi Layanan Teknologi Informasi. *Nuansa Informatika*, *17*(1), 169–178. https://doi.org/10.25134/fkom%20uniku.v17i1.7233

Priyadi, Lingga, Saedudin, R. D. Rohmat, & Fauzi, Rokhman. (2019). Penerapan Manajemen Layanan Teknologi Informasi Pada Pt Albasia Nusa Karya Dengan Menggunakan Framework Itil Versi 3 Pada Domain Service Design. *EProceedings of Engineering*, *6*(1).

Priyohutomo, Andreas Niko, & Sitokdana, Melkior Nikolar Ngalumsine. (2020). Dampak Implementasi Iso/Iec 20000 Pada Perusahaan Pt. Visionet Data Internasional. *Sebatik*, *24*(1), 29–36.

Ramadhan, Reo Ramalika. (2019). *LAPORAN KERJA PRAKTEK di PT. FASA CENTRA ARTAJAYA*.

Romadini, Suci, Santoso, Ari Fajar, & Santosa, Iqbal. (2018). Perancangan Sistem Manajamen Layanan Teknologi Informasi Pada Layanan Reseller Dan Dropship Bandros Menggunakan Iso 20000-1: 2011 Area General Requirements Dan Design And Transition Of New Or Changed Services (studi Kasus: Cv Kabita Informatika). *EProceedings of Engineering*, *5*(2).

Setiawan, Harry, & Sfenrianto, Sfenrianto. (2023). Pengukuran Kinerja Menggunakan ITIL V3 Divisi IT Operation PT XYZ. *Jurnal Informasi Dan Teknologi*, 102–111.

Utami, Setyaningsih Sri. (2010). Pengaruh teknologi informasi dalam perkembangan bisnis. *Jurnal Akuntansi Dan Sistem Teknologi Informasi*, *8*(1).