The 1st International Student Conference on Economics and Business Excellence (ISCEBE) 2024
e-ISSN: xxxx-xxxx/Vol.1 No.1 (2024)

CYBER SECURITY IN OUTSOURCING: STRATEGIES AND TECHNOLOGIES TO MITIGATE DATA SECURITY RISKS IN IT SERVICE MANAGEMENT (SYSTEMATIC LITERATURE REVIEW)

Nada Salsabila Arsy[1)], Asniati Bahari[2)]
[1,2)]Accounting Department, Universitas Andalas, Indonesia
Corresponding author: asniati@eb.unand.ac.id

Abstract

The practice of outsourcing Information Technology (IT) services presents efficiency opportunities, but also increases data security risks due to sharing access with third parties. This study uses the systematic literature review (SLR) method to identify effective risk mitigation strategies and technologies in the context of IT outsourcing. This study collected 25 articles from various journals in the period 2010-2023, The analysis was conducted on literature from leading scientific sources, such as Scopus, IEEE Xplore, and ScienceDirect. The results of the study indicate that IT outsourcing risk management requires a systematic framework such as NIST or ITIL to reduce security risks. Although efficient, the success of outsourcing depends on strategic planning, clear contracts, and risk mitigation. Digital transformation adds to data security challenges that require regulation, awareness, and a holistic approach to protecting organizations.

Keywords: IT outsourcing, Cybersecurity, Effective Mitigation, IT Service Management, Security Technology

Introduction

With the era of digital transformation accelerating the adoption of Information Technology (IT), organizations face significant challenges related to cybersecurity. Business sustainability and data integrity now heavily depend on the capacity of IT infrastructure to defend against increasingly sophisticated cyber threats. Despite advancements in security technology, a deep understanding of the latest methods and techniques to protect digital assets is essential (Hoshmand & Ratnawati, 2023). One strategy that emphasizes collaboration with other companies and is relevant to the current business environment is outsourcing. IT outsourcing refers to a model where companies delegate all or part of planned IT services to professional firms to achieve their objectives.

Good IT Governance is necessary for Telkom to successfully implement the Amoeba project, both for Amoeba and for the company as a whole. According to the Government Information Institute (Baskoro & Kosala, 2020), IT governance consists of five components: strategic alignment, value delivery, risk management, resource management, and performance management. However, outsourcing IT services, particularly IT service management, has introduced new issues regarding cybersecurity. Information system security has become a critical concern in today's digital age. Attacks such as malware, phishing, and insider threats are becoming more complex and often require a comprehensive approach. Data encryption, real-time security monitoring, and employee safety training are some of the key strategies in this regard (Ade Irawan et al., 2024). Cyber attacks, theft or loss of devices, employee data theft or leaks, and human error are some examples of security breaches. SQL injection, cross-site scripting (XSS), and privilege escalation are major cyber attacks occurring in industrial and business systems.

Effective risk mitigation strategies and technologies are crucial in the context of outsourced IT service management. Companies must ensure that their chosen IT service providers have robust security systems and comply with best security standards. They should also establish strict oversight and control mechanisms to minimize cybersecurity risks. This systematic literature review aims to identify, analyze, and synthesize current strategies and technologies used to mitigate data security risks in outsourced IT service management. The urgency of this research is based on the increasing trend of outsourcing IT service management and the complexity of cybersecurity challenges faced by companies. The findings are expected to guide companies in

selecting and implementing appropriate risk mitigation strategies while also providing direction for future research in cybersecurity and outsourcing.

Method

Literature Review Method

To find and select literature relevant to the research topic, the literature review process is outlined in the flowchart. The process begins by searching for literature from databases such as Google Scholar and ResearchGate, which yielded 63 sources.Next, the data is filtered using inclusion and exclusion criteria. Irrelevant sources, such as book chapters, duplicates, reviews, theses/dissertations, and broken links, are removed by Filter 1, leaving 50 sources. The eligibility stage involves further assessment of the relevance and quality of the sources. Filter 2 screens the sources based on more specific criteria, such as publication type (non-SINTA 1-4-7), research focus (implementation, risk assessment, factors, and effectiveness). At this point, 34 sources remain.

Finally, the inclusion stage involves a final screening to select the most relevant and high-quality sources for the literature review. Filter 3 focuses on sources that discuss specific topics such as continuous auditing, software development, and conceptual models, resulting in 25 sources.

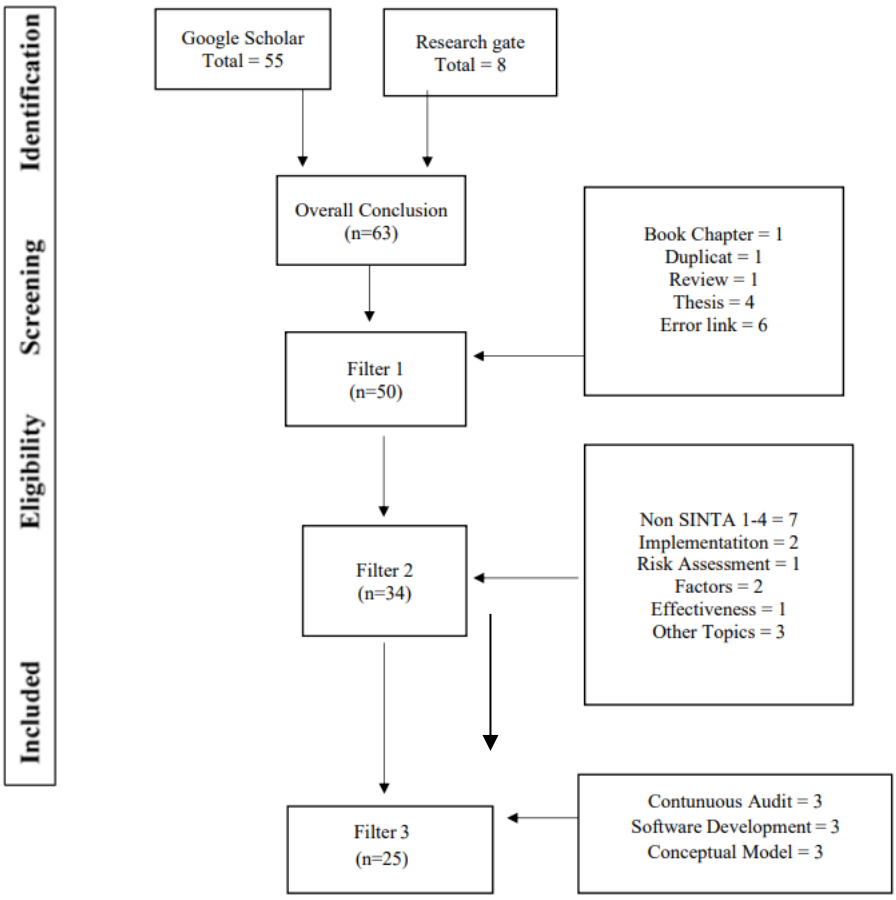

Figure 1.

e-ISSN: xxxx-xxxx/Vol.1 No.1 (2024)

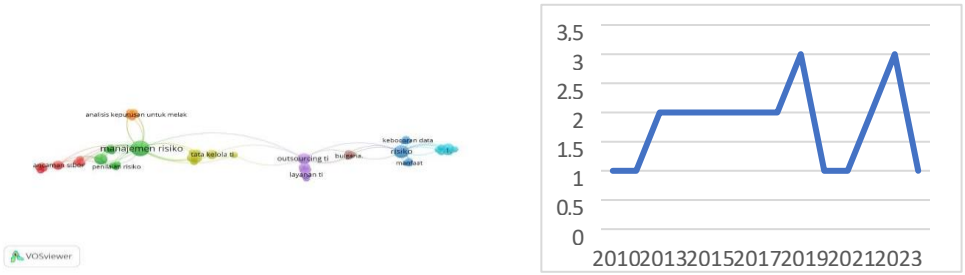

Figure 1. Data Mapping

Using VOSviewer to analyze the topic "Cyber Security in Outsourcing: Strategies and Technologies to Mitigate Data Security Risks in IT Service Management"can provide insights into key keywords, prominent authors, and research trends. Mapping keywords such as cybersecurity, outsourcing, and data security risks can reveal connections between related topics. Additionally, VOSviewer can illustrate collaboration networks among authors and journals that frequently publish research in this field. By mapping data from sources like Reaserch gate and Google Scholar, VOSviewer can also help identify emerging research trends and technologies used to mitigate security risks in IT service management.
The distribution of articles over time, as illustrated in Figure 2, spans the period from before 2014 to 2024. The data reveals a noticeable increase in research on outsourcing. This upward trend indicates that outsourcing has been receiving growing attention from academics and researchers in recent years. Given the progression of published articles and the sample of studies examined, this trend suggests that outsourcing remains a significant and evolving topic in the field of business strategy, IT management, and global economics, warranting continued exploration and investigation. The rising focus on outsourcing reflects the increasing complexity of outsourcing decisions, including considerations around technology, security, vendor management, and regulatory compliance.

Results and Discussion

Table 2. Framework for System Acquisition

No	Methods & Study Topics	Article
1	Framework for System Acquisition	(Fahrudin et al., 2022) , (Gritzalis et al., 2007) , (Coccio, 2012)
2	Technology Acquisition Decisions	(Dhar, 2014) , (Algarni, 2021)
3	Framework Based Service Management	(Uddin, 2014) , (Keamanan, 2018)
4	Security and Privacy in Service Management	(Hoshmand & Ratnawati, 2023) , (Delima Sari, 2023) , (Ade Irawan et al., 2024)
5	Service Evaluation and Optimization	(Cruz et al., 2013)
6	Outsourcing Strategy	(Ravi et al., 2023) ,(Anjar, 2005)
7	Outsourcing Risks and Mitigation	(Baskoro & Kosala, 2020) , (Arshad, 2014) ,
8	Security and Outsourcing Policy	(Patel, 2024) , (Cryptocurrency et al., 2021)

According to the literature review, there are 3 articles that discuss the Framework for System Acquisition. According to research from (Fahrudin et al., 2022) NIST SP 800-30 provides a structured and orderly approach to managing IT system security risks by identifying, assessing, and mitigating them. The process consists of risk assessment, mitigation, and evaluation of controls, wherein threats are identified and assessed for their likelihood and impact. The mitigation measures involve data backups, updating antivirus, and restriction of access, among others, while the evaluation is done periodically to ensure that controls are effective. Analysis shows that the major threats are human error, hacker attacks, and technical failure, which can be prevented by disaster recovery plans, training of employees, and updating procedures. Good documentation supports audits and managerial decision-making. (Gritzalis et al., 2007) This probabilistic model is designed to

develop optimized insurance contracts for managing security risks and privacy breaches in IT outsourcing. This model will help organizations in addressing such threats, like data leakages, by financially supporting them with fair compensation while maximizing the company's satisfaction by utilizing utility functions concerning the different scenarios of a security incident. Aside from protection, this model urges the contractor to uphold his or her integrity to support decisions for acquiring much safer and more efficient systems. (Coccio, 2012) The challenges faced by the DoD in managing acquisition workforce to support military operations, especially during the wars in Iraq and Afghanistan, are significant. On the other hand, when dependence on external contractors is higher, violations of core competencies and lesser institutional control are common phenomena. To deal with this, the DoD uses an approach that separates functions according to their criticality, meaning governmental functions must be performed by internal personnel, while commercial functions can be outsourced, but under strict oversight. Nonetheless, difficulties in losing institutional control and shortages of the internal workforce, coupled with failures in managing the contract, do arise. To remedy this, DoD improves the training and certification of the workforce through institutions such as the Defense Acquisition University, DAU, and creates agencies such as the Defense Contract Management Agency, DCMA, to better manage contracts. This approach is designed to effectively incorporate risk analysis into the system acquisition process for operational efficiency and sustainability.

Technology Acquisition Decisions

According to research (Dhar, 2014) Technology acquisition decisions are very crucial in corporate management, which involves a careful analysis of impacts, challenges, and implementation strategies. The positive impacts are improved efficiency, innovation, and competitiveness, while the challenges are cultural integration, resource limitations, and uncertainties. Some of the key factors that influence the decision to acquire technology include information quality, management experience, and market trends. Effective strategies to address challenges include due diligence, structured integration plans, and stakeholder engagement. The acquisition of PT Supra Boga Lestari Tbk by Blibli illustrates how technology and AI can be used to manage the benefits and challenges of technology acquisition. This review emphasizes the role of technology acquisition in ensuring corporate success..(Algarni, 2021) Technology acquisition decisions are very important in terms of organizational growth and efficiency. Some key factors to be considered include analysis of the needs of the organization, available resources, and associated risks, such as cybersecurity threats. The decision-making process involves detailed due diligence and stakeholder participation, while implementation strategies, including integration plans and employee training, are necessary for successful execution. Case studies provide practical insights into challenges such as resistance to change and cultural issues. Decisions are also influenced by considerations of future trends in AI, IoT, and big data. The review thus gives strategic directions to organizations in an effort to navigate challenges and optimize success with regard to technology acquisition.

Framework Based Service Management

(Uddin, 2014) Service management frameworks, including ITIL, COBIT, and ISO/IEC 20000, have bettered IT service management by allowing organizations to improve service quality, operational efficiency, and customer satisfaction. These frameworks direct guidelines for key processes in incident, problem, and change management. Challenges include organizational resistance and resource limitations. Case studies provide practical benefits and lessons; trends such as automation, AI, and data analytics shape the future of service management. Such frameworks have been consistently successful and performance-appropriate through proper metrics and KPIs. Overall, this overview is done on benefits, challenges, and strategies that improve service management in organizations..(Keamanan, 2018) Service management based on frameworks involves the use of structured approaches, such as ITIL, COBIT, and ISO/IEC 20000, in order to provide quality IT services. These frameworks enhance service quality, operational efficiency, and customer satisfaction by applying various processes, including incident, problem, and change management. Challenges to implementation include resistance to change and resource limitations. Case studies offer insights into successful adoption, while emerging technologies like automation, AI, and data analytics enhance efficiency. Performance evaluation by metrics and KPIs enables continuous improvement. The following review gives an overview of framework-based service management, its benefits, challenges, and strategies for improving IT services.

Security and Privacy in Service Management

(Hoshmand & Ratnawati, 2023) Security and privacy are vital in service management to protect sensitive data through encryption, access controls, and audits. Network and application security prevent threats, while data privacy must comply with regulations like GDPR. Risks such as cyberattacks and data breaches can harm reputation and trust. Key strategies include clear security policies, privacy training, and regular risk assessments. Encryption and cybersecurity solutions provide improved protection, but the challenges include resource limitations and changing regulations. Case studies provide insight, and emerging technologies such as AI and blockchain are influencing future practice. This review provides a comprehensive guide to managing security and privacy in service management.(Delima Sari, 2023) Security and privacy reviews in service management show the importance of protecting data and systems. Security protects against unauthorized access and threats, while privacy ensures individuals are in control of their personal information. Both are crucial in ensuring customer trust, reputation, and regulatory compliance. Frameworks such as ISO/IEC 27001 and GDPR help with managing these aspects. Threats include cyber-attacks, data breaches, and human errors. Best practices include access control, encryption, and audits on a regular basis. Protection is enhanced by the use of emerging technologies such as AI, data analytics, and blockchain. Challenges involve limitations in resources and training; future trends are toward adapting to increasing stringency in regulations and technological changes.

(Ade Irawan et al., 2024) Security and privacy in service management focus on the protection of data and systems against vulnerabilities, with the ability of individuals to maintain their personal information. Both are important features of customer trust, reputation, and compliance with the law, the failure of which might bring financial and reputational losses. Such policies are informed by frameworks like ISO/IEC 27001 and GDPR. Security threats include cyber-attacks and data breaches, mitigated through risk assessments, access management, encryption, and employee training. This makes emerging technologies like AI and data analytics enhance security while challenges include resource limitations and regulatory complexity. Case studies present several best practices for insight, while the influence of evolving regulations and technological advancement determines future trends.

Service Evaluation and Optimization

(Cruz et al., 2013) Service evaluation and optimization are essential in the realization of better quality and efficiency of service. Evaluation involves assessing effectiveness, efficiency, and quality through methods like surveys, audits, and performance analysis, using KPIs such as response time and customer satisfaction. It aims at ascertaining areas for improvement and ensuring compliance. Service optimization has to do with cost reduction, quality enhancement, and customer experience through strategies such as technology adoption, employee training, and process improvements like lean management and Six Sigma. These are enabled by emerging technologies such as AI and big data. Challenges involve limitations in resources, resistance to change, and outcome measurement; hence, effective management strategies will be required.

Outsourcing Strategy

(Ravi et al., 2023) Outsourcing strategies are those in which business functions are delegated to third-party vendors with the aim of enhancing efficiency, cutting costs, and concentrating on core competencies. Goals include cost savings, access to expertise, flexibility, and strategic focus. Types of outsourcing include BPO, IT outsourcing, and manufacturing outsourcing. In choosing the right vendor, one has to consider reputation, experience, cost, and technical capabilities. Success depends on effective communication, collaboration, and goal-setting. Performance monitoring and contingency planning will help mitigate risks like loss of control and dependency on the vendor. Technologies that enhance outsourcing include cloud computing and automation, while resistance to change and system integration pose some challenges. Nearshoring, new technologies, and sustainability are some of the future trends.(Anjar, 2005) Outsourcing strategies involve transferring certain functions to third-party providers in order to reduce costs, increase efficiency, and focus resources on core competencies. These include BPO, IT outsourcing, and manufacturing outsourcing. Goals include gaining specialized expertise, flexibility, and adapting to market changes. To select the right vendor, one must evaluate reputation, experience, and costs with risk assessments. Outsourcing models, such as total, selective, and transformational outsourcing, have different advantages. Successful outsourcing depends on effective vendor management, clear contracts, and performance monitoring. Controllable risks include loss of control and data security, which can be mitigated by developing contingency plans. Technologies like cloud

computing and automation enhance outsourcing, while challenges like employee resistance and system integration can be addressed with the right strategies. Future trends include nearshoring, new technologies, and a focus on sustainability.

Outsourcing Risks and Mitigation

(Baskoro & Kosala, 2020) Outsourcing risk and mitigation involve the management of problems arising in the performance of tasks by third-party vendors. The main risks are strategic risks, such as poor choice of vendors; operational risks, including those that concern vendor relationships and service quality; financial risks related to unexpected costs; and legal risks regarding compliance. Risk identification is done using methods such as SWOT analysis and stakeholder surveys, while a risk matrix prioritizes risks. Mitigation strategies include vendor diversification, clear contracts, performance monitoring, and employee training. Effective vendor management is important, and trends for the future include analytics and automation. Case studies have provided insight, while best practices minimize issues and optimize outsourcing benefits.(Arshad, 2014) Outsourcing risks and mitigations involve understanding the potential issues that arise by delegating functions to third parties. These include strategic risks, such as poor selection of vendors; operational risks regarding relationship management and service quality; financial risks, such as unexpected costs; and legal risks, such as non-compliance. The identification can be done through SWOT analysis, stakeholder interviews, and surveys. Risk prioritization can be done by using a matrix. Some mitigation strategies include vendor diversification, clear contracts, monitoring performance, and employee training. This also involves effective vendor management and how to overcome challenges such as resistance to change. Future trends will include data analytics and automation. Case studies provide insight, and best practices show how to maximize the benefits while minimizing the risks of outsourcing.

Security and Outsourcing Policy

(Patel, 2024) The meaning of security in outsourcing deals with data protection, the integrity of systems, and physical and informational security where third-party services are contracted. The major risks it faces include data breaches, cyber-attacks, and compliance failure by vendors. A really robust security policy should spell out all details on vendor security standards, procedures for incident response, employee training, security clauses in all contracts, audit rights, security monitoring and threat detection technologies, efficient and amiable relations with vendors, and associated communication. Challenges like resistance from vendors and regulatory complexity require appropriate management strategies. Future trends focus on AI for threat detection and cybersecurity. Robust security policies are very much necessary to safeguard organizational data and systems.(Cryptocurrency et al., 2021) Outsourcing security concerns data, system integrity, and asset security with the third-party provider. There are threats of data breaches, cyber attacks, and challenges concerning vendor compliance. A direct security policy is necessary on standards, incident response, and employee and vendor training. There should be contract clauses with audit rights inclusive. Technologies that detect threats should be instituted through the monitoring process and should relate to good relations with the vendors and communication with them. The challenges in implementation, such as resistance by vendors and regulatory issues, require effective strategies. Future trends are AI for threat detection and a focus on cybersecurity. A strong security policy is crucial to protect data and systems.

Conclusion

This literature review highlights the critical importance of managing cyber security risks in outsourcing, particularly in the context of IT service management. The research shows that outsourcing involves significant security risks, including data breaches, cyberattacks, and vendor non-compliance with regulations. To address these challenges, developing a comprehensive security policy is essential, which includes vendor security standards, incident response procedures, as well as training and awareness programs for both employees and vendors.

Technologies and strategies used to mitigate security risks in outsourcing include encryption, access control, audits, and advanced technologies like artificial intelligence (AI) and blockchain to detect threats and enhance data protection. Furthermore, continuous security monitoring and effective vendor relationship management are emphasized as crucial factors in minimizing risks.

The review also identifies implementation challenges, such as resistance to change, resource limitations, and regulatory complexities, which can hinder the success of security policies. Therefore, careful management,

including training, strong policy integration, and well-prepared contingency planning, is necessary for effectively managing these risks.

Overall, robust security policies, supported by cutting-edge technology and efficient vendor management, are key to ensuring successful and secure outsourcing in IT service management.

Reference

Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, & Fried Sinlae. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. *Journal Zetroem*, *6*(1), 114–119. https://doi.org/10.36526/ztr.v6i1.3376

Algarni, A. M. (2021). *terapan Penilaian Kuantitatif Risiko Keamanan Siber untuk Mitigasi Pelanggaran Data dalam Sistem Bisnis*.

Anjar, P. (2005). Operasional Teknologi Informasi Yang Efektif Dengan Outsourcing. *Seminar Nasional Aplikasi Teknologi Informasi 2005*, *2005*(ISBN: 979-756-061-6), 7–9.

Arshad, N. H. (2014). *Kerangka Konseptual Manajemen Risiko dalam Outsourcing TI Proyek*.

Baskoro, H., & Kosala, R. (2020). Identifikasi Risiko dari Outsourcing IT. *Jurnal Sistem Informasi Bisnis (JUNSIBI)*, *1*(2), 73–79. https://doi.org/10.55122/junsibi.v1i2.174

Coccio, K. K. L. (2012). *Outsourcing , Insourcing , dan Mempertahankan Akuisisi Profesi Tenaga Kerja*.

Cruz, A. M., Maria, A., Rincon, R., & Haugan, G. L. (2013). *Mengukur Kinerja Outsourcing Layanan Pemeliharaan*. 524–535.

Delima Sari, S. (2023). Privasi dan Keamanan Data Dalam Statistik Resmi: Tantangan dan Solusi Dalam Perlindungan Data Individu. *Jurnal Ilmiah Multidisipline*, *1*(11), 700–703. https://doi.org/10.5281/zenodo.10371661

Dhar, S. (2014). *Risiko , Manfaat , dan Tantangan dalam Outsourcing TI Global : Perspektif dan Praktik*.

Fahrudin, N. fitrianti, Nugraha S, A., & Ramadhan Putra, K. (2022). Penilaian Risiko Keamanan Data Karyawan Pada Sistem Informasi Dengan Menggunakan Framework Nist Sp 800-30 pada PT. ABC. *Jurnal Ilmiah Teknologi Infomasi Terapan*, *8*(3). https://doi.org/10.33197/jitter.vol8.iss3.2022.900

Gritzalis, S., Yannacopoulos, A. N., Lambrinoudakis, C., Hatzopoulos, P., & Katsikas, S. K. (2007). A probabilistic model for optimal insurance contracts against security risks and privacy violation in IT outsourcing environments. *International Journal of Information Security*, *6*(4), 197–211. https://doi.org/10.1007/s10207006-0010-x

Hoshmand, M. O., & Ratnawati, S. (2023). *AIKOM Teknologi Informasi Terapan dan Ilmu Komputer Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Keamanan Siber Ancaman*. *2*(2), 9–18.

Keamanan, P. (2018). *Jurnal Teknik Sistem Informasi dan Intelijen Bisnis Manajemen Strategis untuk Layanan TI pada Outsourcing Perusahaan Keamanan*. *2555*(1), 46–56.

Patel, Y. (2024). *Keamanan & Kepatuhan Dalam Mengelola Produksi Lingkungan*.

Ravi, A., Donawa, N., & West, P. (2023). *Pentingnya Outsourcing Strategis dalam Manajemen Proyek TI Pentingnya Outsourcing Strategis dalam Proyek TI Pengelolaan*.

Uddin, B. (2014). Evaluasi Penerapan Manajemen Layanan Ti Menggunakan Kerangka Kerja It Infrastructure Library (Itil) Sub Domain Service Desk, Incident Management, Dan Problem Management Pt. Xyz. *Tedc*, *8*(2), 171–177.