THE DYNAMICS OF USING THE MOBILE CONTROL RAPID REPORTING SYSTEM APPLICATION (SIPACE TROLLING) AT THE CLASS IIA MADIUN YOUTH CORRECTIONAL INSTITUTION

Uchox Alvyanus Hutapea

Program Studi Manajemen Pemasyarakatan, Politeknik Ilmu Pemasyarakatan – Indonesia

e-mail:
uchoxhutapea74@gmail.com

ABSTRACT

Adopting technology in digital security systems requires adequate skills and knowledge for security management to achieve its objectives, which are to create conducive conditions, maintain officer order, and ensure prison safety. This research aims to ensure that organizations can identify, measure, and monitor the various risks that may arise from the application. This research uses a qualitative method with a descriptive approach by conducting in-depth interviews with correctional officers at the Class IIA Madiun Youth Correctional Institution who serve as structural and executive officials. From the risk identification, the results obtained from the four risk points that have been described can be an important concern for the organization in operating the application. From those with a high-risk value to those with the lowest risk value, all must get risk treatment because risks can interfere with the organization's running if the organization is not handled properly.

Keywords: *Application; Risk Management; Prison*

INTRODUCTION

Indonesia is currently undergoing a deep and comprehensive transformation. This change encompasses various aspects and sectors, with the aim of improving shared prosperity and prioritizing the public interest. Whether prepared or not, and regardless of approval or rejection, every organization is expected to make fundamental and systematic improvements in the way it thinks and acts in managing its operations. In the context of organizations, this arrangement gives rise to various options or innovation designs. The rapid development of technology certainly plays a significant role in supporting various human activities and activities, including in the context of the State Civil Apparatus (ASN) bureaucracy in carrying out its main duties and functions. Quoting a statement from Read Brain (1937), explains that a technology is generally objects that can be used or felt by humans to support or support their lives to make various updates in the present and future era. (Pasya & Wibowo, 2022).

Several recurring narratives are always brought to the public regarding the system and conditions of prisons and detention centers. Overcrowding is a long-standing unresolved issue in prisons and detention centers. Overcrowding itself can cause other problems, such as disturbances to security and order. According to data compiled from the LAKIP (Laporan Akuntabilitas Kinerja Instansi Pemerintah) Directorate General of Corrections in 2022, there are 526 prisons and detention centers in Indonesia with an overall capacity of 132,107 residents. The current number of inmates in Indonesian prisons and detention centers in 2022 has reached 275,167 inmates.

Table 1
Table of disturbances in the Directorate General of Corrections

Year	Escaping	Narcotics	Riots, fights, assaults and violence	Others
2019	31	84	10	7
2020	29	111	7	10
2021	17	22	0	0
2022	37	106	0	1

Source: Directorate General of Corrections Performance Report 2019 - 2023

The graph shows that the conditions of security disturbances that occur in prisons and detention centres throughout Indonesia show fluctuating data (up and down conditions). It can also be concluded that an optimal solution has not yet been found in preventing the existing security disturbances.

In 2023, the Corrections Division of the Regional Office of the Ministry of Law and Human Rights of East Java Province received 15 complaints related to violations of security and order in prisons and detention centres. Most of the complaints received about security and order disturbances by WBP (Prisoners of Correction), namely the use of narcotics and cellphones in prisons and detention centres in the East Java Regional Office. The majority of WBP involved in these offences are generally drug offenders. They try to use various smuggling methods in order to consume drugs in prison. Not a few of them are also involved in smuggling mobile phones so that they can have a network in controlling drugs, and can also build networks from parties outside the prison or detention centre.

Based on the description of the data above, during the period 2023 in the East Java Regional Correctional Unit, the largest number of complaints fell on the UPT in the Madiun regional office (regional coordinator). Complaint data shows that Madiun Youth Correctional Facility received the most complaints. From the overall data also shows the

existence of kamtib disturbances originating from mobile phones or mobile phones (cellphones). Basically, the security function in prison plays an important role in providing a sense of security to prisoners, detainees, and correctional children. When associated with the concept of security in security management itself quoted from the statement of Sheryl Strauss (1980: 1), the concept of security refers to preventive action against various forms of losses that may arise from various causes. The role of management has great significance in realising organizational goals, especially in the context of prisons where management in security plays a crucial role in supporting the implementation of optimal and adequate coaching programs in prisons.

From the description of the problem, there is pressure to make some changes to the way of working or the system of the organization itself. The leaders try to rack their brains or realise an innovation so that the wrong work culture becomes back according to what is expected by the organization's goals. Security administration management at Class IIA Madiun Youth Correctional Facility has been running effectively, but the creation, management and archiving of security reports are still carried out conventionally. In this regard, the prison made a breakthrough or innovation in the form of utilising Information Technology (IT) through a change action project with a Near Field Communication (NFC) Android-based application through the Mobile Control Quick Reporting System (Sipace trolling) which is directly connected to the leadership to supervise, monitor the implementation of mobile control of security officers in prisons. From the utilisation of technology, researchers see the problems that arise through two sides. The first side is the reason for the use of digital roving control and the second side is the application used.

To face challenges and threats in order to achieve goals, planning is an important element in implementation. In this process, risk management can be integrated into management planning. The main objective of risk management is to ensure that the organization can identify, measure and monitor various risks that may arise. In addition, risk management aims to ensure that the policies implemented are able to handle all types of risks. For example, in the use of technology in prison security systems, it is important to anticipate risks that may arise in the future related to the applications used. This includes how it is maintained, handled in case of damage, misuse, and acceptance or resistance from the environment, both officers and prisoners. These environmental influences will impact the future operation of the application.

Based on the facts and data previously described, the adoption of technology in digital security systems requires adequate skills and knowledge for security management to achieve its goals of creating conducive conditions, maintaining officer order, and ensuring prison safety. In addition, it is important to understand the risks that may arise in order to design preventive measures against future applications.

LITERATURE REVIEW

Research from Pasya and Wibowo (2022) focuses on how technology affects the implementation of existing tasks and functions, as well as providing various benefits through application-based technological innovations, both those developed by the Ministry of Law and Human Rights, the Directorate General of Corrections, as well as service application innovations produced by the Muara Enim Class II B Penitentiary itself. The results show that the Class II B Muara Enim Correctional Institution has optimally utilised Information Technology in carrying out its duties and functions. This is evidenced by the use of various application-based technologies designed to facilitate the implementation of tasks, as well as directly monitor the activities carried out to prevent

fraud and ensure the fulfilment of the rights of prisoners, detainees and children. Thus, coaching can be carried out in accordance with the objectives that have been set.

Research from Salim and Prasetyo (2023) focuses on reviewing the risk management design that is in accordance with the characteristics of the Company in the process of achieving the vision and mission of the company, as well as conducting a risk assessment for the Company. This research identifies the company in each part to take mitigation steps for future organizational needs. Therefore, it is necessary to form a risk management working group to assess the suitability and accuracy of existing risks.

Sandhyavitri and Young (2004) revealed that risk management involves a series of planned steps, such as planning, identification, analysis, response actions, and monitoring of risks that may arise in projects. Sandhyavitri also explained the main elements in risk management, namely (1) Development of basic models for financial calculation; (2) Risk Analysis; and (3) Risk Mitigation. Then developed again in his research into (1) Risk Identification; (2) Risk Analysis and Assessment; (3) Risk Mitigation and Control; and (4) Risk Management (Sandhyavitri & Saputra, 2019). According to Smith (1990), Risk Management is the process of identifying, measuring, and controlling financial risks that may threaten the assets and revenues of a company or project, with the potential to cause loss or damage. In this article, Smith discusses the theory that explains how risk management mechanisms can increase the value of an organization. The researcher believes that this is an important first step in designing an effective risk management program. This theory is used by the researcher to explain how the risks and impacts of implementing a digital security system can affect operations within prisons. The researcher uses four main elements in risk management which include, risk identification, risk analysis, risk evaluation, and risk handling.

METHOD

This research uses a qualitative method with a descriptive approach. Qualitative research is a type of research that originates from an inductive approach, where this research is based on objective and participatory observation of a social phenomenon (Suyitno, 2021). According to Moleong (2005: 6) in Fattah (2023), qualitative research can be explained as a research method that aims to understand specific phenomena, such as behaviour, perceptions, motivations, actions, and other things experienced by research subjects. The informants of this research are correctional officers at the Class IIA Madiun Youth Correctional Institution who serve as structural and executive officials. There are 5 correctional officers who were successfully interviewed by researchers directly. With a total of two officers with positions as Section Head of Security Administration and Order and Head of Prison Security Unit (KPLP). Primary data were obtained through in-depth interviews, while secondary data were collected from literature studies and related documents, such as journal articles, regulations, and personnel documents. Afterward, relevant data were selected and verified through data triangulation before being presented as a discussion theme.

RESULTS AND DISCUSSION

Factors driving the use of the Sipace Trolling application

Before discussing the research questions, the researcher will first explain the factors that drive the implementation of digital control in Madiun Youth Correctional Facility, which then results in the Sipace trolling application as a tool to support the supervision of the security team in the prison. In general, roving control is a preventive measure in maintaining security in prisons and detention centres. The rules regarding this guarding

have been regulated in the Penitentiary Guarding Regulation Number: DP.3.3/17/1 on 27 January 1975. Responsibility for security and order within the prison rests with the head of the work unit, with the support of the head of security and the guard team.

Not optimising the guarding team in carrying out their duties will result in the failure of the absolute requirements of coaching, namely safe and orderly prison conditions. Carelessness or negligence of the guarding team will provide an opportunity for prisoners to commit irregularities. The same thing was also conveyed by Kasi Adkamtib Lapas Pemuda Madiun as a pilot project from the birth of the application to the ratification by the head of the prison to implement the guard team in the prison.

> *"...nah buktinya ngga ada. Hanya tulisan di kertas, di buku laporan, kontrol Blok A, kontrol Blok B, untuk bergerak apa tidaknya kan kita nggak tahu. Entah nanti anggota disitu Cuma nulis aja, duduk, nanti tulisnya kontrol..."*
> (interview with Kasi Adkamtib, 5 April 2024)

From this excerpt, Pak Agung describes Rupam's sub-optimal performance in carrying out its duties and functions in the field. Rupam carried out their duties only to the extent of fulfilling their obligations by completing the guard administration which was filled in to prove that they had carried out their duties. Pak Agung observed that as long as he was the direct supervisor of Rupam, Rupam only filled in the control book but did not carry out roving controls which should be carried out to observe the situation and conditions of the environment and prison security. The lack of awareness of the Head of the Security Squad (Karupam) and members of Rupam in carrying out mobile control activities in the context of early detection of security and order disturbances in the prison has always been the origin of the disturbance itself.

Then, another factor expressed by Mr Agung which is the driving force to implement this application is the lack of strong evidence that rupam has carried out control, the excerpts are as follows

> *"...Kan dari situ kan nggak kuat melaksanakan tugas, bukti otentik kita itu nggak kuat. Apalagi kalau tidak kontrol sama sekali. Harusnya di jam dua belas itu kontrol, dia nggak kontrol dan ternyata disitu ada yang berantem, ada yang sakit, dan yang sakit meninggal. Nah ketika diperiksa, kamu kontrol nggak? Itu sakit jam berapa itu?..."*
> (interview with Kasi Adkamtib, 5 April 2024)

The function of evidence referred to by Mr Agung, it can be interpreted into two, namely evidence as having carried out the task so that superiors can know directly that their ranks have carried out their duties properly. The second is evidence as having carried out the task that when an incident occurs, be it a disturbance of kamtib, the physical condition of prisoners, the physical condition of buildings and buildings, and other conditions, and when an examination is needed, Rupam can explain with strong authentic evidence that they have actually carried out their duties at the place and time proven in real-time by digital applications or program.

Based on the problem-solving analysis, it is found that the problem that will be raised by the pilot project in this action of change is the suboptimal implementation of the security team's duties in early detection activities and roving control activities in areas considered prone to security and order disturbances. In this case, researchers try to prove whether it is true that violations of the rules in the prison are still not under control. Researchers when examining data on violations of discipline found and documented a

copy of the F register which contains data and information on the list of prisoners who committed violations of discipline and found the following data:

Table 2
Table of disturbances in Class IIA Madiun Youth Correctional Facility

Month	Kamtib Disturbance Data
January	147
February	118
March	49
April	188
May	54
June	178
July	90
August	147
September	112
October	121
November	33
December	8

Source: Adkamtib Section, processed by researchers, 2024

From the copybook of the Register F data, information was obtained that the display contained four months of recap data with a total list of 274 offenses. From this total, it is found that (1) In September there were 112 lists of violations (2) In October there were 121 lists of violations (3) In November there were 33 lists of violations (4) and in December there were 8 lists of violations. The data supports the results of Mr Agung's analysis that it is true that before the application was implemented, the data on violations of prisoner discipline was still relatively high.

Researchers also obtained information when the Sipace Trolling application was first formed, it was still a barcode scan system. And then the idea arose to facilitate the process and of course more practical to use, in the end the system in the application was changed to NFC (Near Field Communication) based. NFC (Near Field Communication) is the latest technology for data transfer based on RFID (Radio Frequency Identification), using wireless connectivity. This technology allows data communication between electronic devices in close proximity by utilising the magnetic field induction present on the device. NFC works within a radius of about 4cm and provides a wireless connection between your device and another device. (Djamar et al., 2017).

The information obtained by researchers when Mr Agung had finished carrying out PKP and planned to implement it into Madiun Youth Prison and was welcomed with good and full support from the Head of Madiun Youth Prison, Mr Ardian Nova Christiawan. Mr Agung also said that rupam responded positively and supported if the application could be implemented. Then the researcher received information if the decree on the determination of the application was issued and finally as of 1 November 2023 sipace trolling began to be activated until now. Pak Agung conveyed information to the researcher that the head of the prison wanted the copyright to be made immediately, because it was at risk of being plagiarised and used by others to become property.

Source: processed by the researcher, 2024

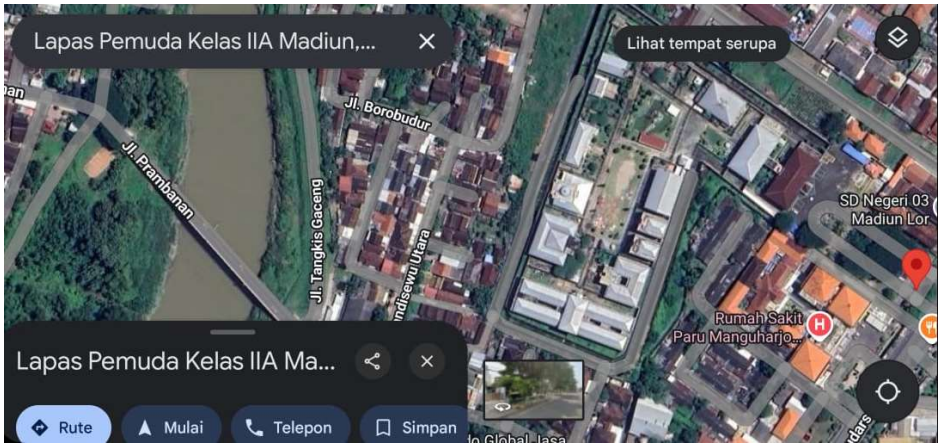
Figure 1
Sipace Trolling Application View

In the background of the birth of the sipace trolling application, guard officers' undisciplined duties and functions is one of the root causes of the problem analysed by Pak Agung as the pilot project and the main informant in writing this research. The lack of awareness of Karupam and Rupam members in carrying out trolling activities in the context of early detection of security and order disturbances in prisons is one of the problems raised as the background of the application. Mr Agung, the main informant, believes his analysis statement is based on his findings in the field during his time as a correctional officer and served as the head of KPLP at that time. Before his current position, Mr Agung held the position of Head of KPLP at Class IIB Sumedang Correctional Facility.

In carrying out his duties and functions, Pak Agung assumed that the Director General of Corrections' order to echo the three keys to correctional success, one of which is early detection, had not been effective during his tenure. At that time he tried to analyse what was the root of the problem why violations of the rules by prisoners were still relatively high, and had the assumption that the guarding team was not disciplined in carrying out trolling so that there were opportunities and opportunities for prisoners to commit irregularities. And from the results of the interview with Mr Agung, he has an assumption, he thinks that the control book as evidence and supporting data for carrying out control, is only written to fulfil the obligation of the guard on duty. This is what is a vulnerability in duty according to him. Because we ourselves as superiors do not know when an incident or problem will occur.

In the opportunity for researchers to conduct research on the use of the application, researchers obtained several important notes from Rupam's information as long as they carried out their duties and responses to the existence of this application implemented in correctional institutions. Several informants interviewed admitted and had in common that they confirmed that the trolling that was running was ineffective, trolling was only carried out by filling out the administration which was considered an important obligation and priority when the leadership conducted an inspection of the duties and functions of Rupam. From the statement of Karupam and Wakarupam during the interview with the quote above, it is similar that they gave their responses regarding

the lack of existing security teams. Based on observation records, Madiun Youth Correctional Facility itself has a building area of approximately 42,820 M^2.



Source: Google Maps, processed by the researcher, 2024

Figure 2
Aerial View Photo of Madiun Youth Correctional Facility Plan

These notes show that Madiun Youth Correctional Facility is a very large physical building area. From the description of the prison area above, it is also illustrated that the prison area forms a letter L, where the upper tower post must still be filled with good judgement even with a small number of members. This is the main dilemma for them as rupam and must continue to carry out their duties with the rules. In the author's observation notes, it was also noted that rupam, in one guard shift, only contained five people including Karupan and his members. This factor is the reason why they are not disciplined in carrying out trolling according to the SOP.

As for the meaning of digitalisation to create a clean, effective, transparent, and accountable governance system and quality and reliable public services, an electronic-based governance system is needed. (Veronica et al., 2022). When discussing performance and the achievement of organizational goals, this cannot be separated from the individuals who run the system in the organization, namely humans. Humans play a role in driving and changing the system and work culture of the organization. With digitalisation, applications are used as a tool to help organizations or agencies monitor the performance and discipline of officers. This allows organizations to have high-quality human resources. In the process, digitalisation will not always run perfectly, because basically technology is also made by humans themselves, there will always be errors either from machines or humans themselves in operating technology. Risk management can be a way to take mitigating steps in adopting technology for organizations.

Risks in Using Sipace Trolling

In risk management theory, Smith (1990) revealed that risk management mechanisms can increase the value of an organization. This theory is used by researchers to be able to explain or explain how the risks of and work from the process of the digital security system into the prison. Risk identification is the earliest stage in the process. Risk identification itself includes determining potential risks and understanding their characteristics. In the risk identification process, there are three main aspects that need to be understood, namely knowing the existence of risks, understanding the causes of the emergence of risks, and understanding the methods used to identify risks and their

causes. Based on the results of the research conducted at the Madiun Youth Correctional Facility, the researchers obtained an outline of several risks obtained from observations in the field and interviews conducted by researchers to the guard executor and several officials directly related to the application, and obtained the potential risks based on the description below.

The first is the legal basis for using the application. Basically, the use of the application is not in accordance with the procedures or legal basis related to the security and order of correctional institutions or detention centres. That every inmate or detainee is prohibited from owning, carrying and / or using a communication device, and the presence of officers carrying communication devices into the block area can potentially lead to irregularities in the form of exchanging interests. This has also been regulated in the Decree of the Director General of Corrections of the Ministry of Law and Human Rights of the Republic of Indonesia Number: PAS-416.PK.01.04.01. 2015 concerning Standards for the Prevention of Security and Order Disorders in Prisons and Detention Centres in the context of controlling communication equipment, officers are prohibited from using personal communication devices in the form of mobile phones or the like to be used in the residential block environment. However, Mr Agung continues to carry out or implement the application on the basis that he has made an SOP and a mutual agreement that mobile phones are only used specifically for the implementation of mobile control using sipace trolling.

The second is Application Supervision and Maintenance. The results of researchers' notes in the field also show that the NFC Sipace trolling box is not included in the BMN inventory list in the office or prison. Because at the time of making the application, all of it used financial assistance from CSR or third parties from the prison, so it has a potential risk of being lost or stolen or damaged without supervision or without strict monitoring from the office administration or it can be called irresponsible damage. The third is Application Copyright. Based on the results of interviews with the pilot project of the application, sipace trolling does not yet have or be registered in copyright. This can be a risk to be imitated or plagiarised similar and the same as the application. And the application itself becomes unenforceable. The last identification is Application Security. Application security referred to by researchers is the security of personal and device data of its users. This was expressed by Rupam as an implementer who had anxiety if he used a privately owned mobile phone to carry out control using sipace trolling. They are worried if their personal data is attacked by malicious components of the application such as viruses or hacking.

From the results of interviews in the field, researchers classified each risk impact, and understood the consequences of the risk. This stage involves assessing the potential occurrence of the risk and the magnitude of the possible impact. The magnitude of the effect can be calculated from two perspectives: likelihood (chance) and impact/effect (magnitude of risk realisation). Then at this stage, the researcher tries to measure the potential risk based on the awareness and knowledge of the five informants the author interviewed about the risks of using the application to measure the magnitude of the existing risk, and obtained. Based on the analysis, it illustrates that the relationship with the legal basis of the application has a higher risk value than other risks. The informants mostly said that the legal basis of the application is still weak and some of them have the same awareness of it. On the other hand, application security is the lowest risk. Most of the informants agreed that the sipace trolling application was safe to use.

Risk Prioritization for using Sipace trolling

At the next stage, after identifying, measuring and estimating the risk of the likelihood of occurrence and the level of risk is risk evaluation. Risk evaluation is the assessment and prioritisation of risks based on their significance and potential impact that may occur. This aims to determine the level of attention that must be given. At the risk level of the legal basis for using the application, it occupies a level with a high level in the previous measurement. Based on the results of researcher interviews, four out of five people have the same awareness that the application still does not have a good legal basis for its use. This is because the application is still carried out with mobile phones that have an internet network for use. This of course contradicts the rule that every officer is prohibited from carrying a mobile phone to enter a sterile area or block area. If an incident occurs, then the use of the application can be a source and assume because it uses a mobile phone for control into the block. When associated with the matrix assessment table, this risk can be placed in the extreme category. Because it has a high probability of risk occurrence, and has the greatest impact on the risk such as the misuse of mobile phones in the block.

In the next potential risk, namely, application supervision and maintenance. In measuring the risk of supervision and maintenance of previous applications, the risk is categorized at a moderate level, because only some of the five informants complained or paid attention to how about maintenance and supervision of application devices. If categorized using the matrix above, supervision and maintenance can occupy a medium position, because it has a relatively moderate possibility of damage, but has high consequences if it is damaged. Then the risk to the copyright of the application can occupy a medium position. Because the application has a low probability of being copied and experiencing plagiarism. But it can have a big impact if it happens. Because if the application itself is exposed to copyright claims, it can make the application mandatory to stop. Therefore, it is classified as having a large impact with a medium risk level. And the last is security. Security itself in the risk category assessed using the matrix above, can be categorized in a low position. Because the concept of the Sipace Trolling application is structured with a minimalist system and a fast process. It can be categorized based on low impact because the application itself, based on interviews with informants, does not show any problems or obstacles in its operation.

Expectations on the use of Sipace Trolling

The next step in the risk management effort is to make a decision on the most appropriate risk treatment option, which involves weighing up the likely benefits that can be achieved in relation to the success of the objective, against the effort or losses that may arise from its implementation. At this stage, of course, those with the highest risk value will receive the highest recommendation for further handling. In general, there are four types of risk control, namely risk avoidance/reduction, risk transfer, risk mitigation, and risk acceptance, while for risks that are viewed from the positive side, in this case, opportunities, the strategy applied is to exploit, share and increase them (Iin et al., 2017).

In the process of approaching the theory with the existing risks in the previous identification, the risk to the legal basis for using the application has the most risky value to the organization. Efforts that have been made during the application are risk mitigation. During the use of the application from the beginning it has been applied or fortified with SOPs in its use. SOPs are issued by the Kalapas to be obeyed by all implementers and officials responsible for the use of applications. However, basically the SOP is also considered insufficient to fortify the legal basis for using the application itself.

This is also supported by the statement of the informant interviewed by the researcher as the pilot project of the application that if an incident occurs which is a violation of the use, smuggling, and misuse of the cellphone used to operate Sipace Trolling, the application will be able to be terminated or abolished because it is considered detrimental to the organization. This is certainly something that is beyond the control of the SOP.

Based on the description of the risk management efforts above, of course we can already describe which ones are a problem, which ones have a high risk, and which ones have the highest priority to be handled further. From the risks above, of course, there is hope from researchers that the application that has been well structured with good goals can have good sustainability in the future. Because with Sipace Trolling, it can reduce the officer's indiscipline in carrying out mobile control which has an impact on the order of prisoners who can be maintained and controlled. Therefore, further risk mitigation steps are needed, which can be in the form of changing the work system or changing the device used to run Sipace Trolling.

The step of changing the work system can be done by changing the application system so that it can be used offline. Using offline can be done by scanning at each control point, then at the end of the control can be integrated online the data stored offline with the computer used to process the data. This system certainly requires the same server and the same IP Address for the connection used during data integration. This system can certainly help reduce the risks of fraud in the operation of Sipace Trolling by implementers in the field. The second is to replace the use of mobile phones with special devices used for Sipace Trolling applications. Or it can be a special HT that can be used to tap and scan NFC on the sipace trolling application. This can certainly minimize the use of mobile phones when carrying out tasks in the field. With these two advanced mitigation steps, it is hoped that the Sipace Trolling application can be maintained even with the existing legal basis.

CONCLUSION AND SUGGESTION

To face challenges and threats in order to achieve goals, planning is an important element in implementation. In this process, risk management can be integrated into management planning. The main objective of risk management is to ensure that the organization can identify, measure, and monitor various risks that may arise. This article discusses the risks that organizations will face in the future and how they will impact the organization. However, with various risks and challenges, with good analysis and policies from the leadership, it is certainly very desirable for the sustainability of the use of existing applications. Digitalization has an important role in the current era, with digitalization human tasks are greatly assisted. But it will be the opposite if we don't use it wisely.

The four risk identification points described above can be an important concern for organizations in operating applications. From those with a high risk value to those with the lowest risk value, all must get risk handling. Because risks can disrupt the running of the organization if the organization is not handled properly. The legal basis for using the application requires further mitigation steps because it has the highest probability and impact on its measurement. Then on maintenance also needs to handle risk reduction in its application. Reduction can be done by registering Sipace Trolling into BMN so that the application can have continued maintenance in its use. Then the other two risk points can be handled by accepting the risk to be given action after handling the previous two risks.

REFERENCES

Creswell, W. J. 2013. Research Design Pendekatan Kualitatif, Kuantitatif, Dan Mixed. Yogyakarta: Pustaka Pelajar.

Creswell, J. W. 2014. Proceedings of the Annual Conference of the International Speech Communication Association

Departemen Komunikasi dan Informatika. 2009. "Cetak Biru (Blueprint) Sistem Aplikasi E-Government Bagi Lembaga Pemerintah Daerah." (9):99.

Djamar, A. S., Sompie, S. R. U. ., & Putro, M. D. (2017). Implementasi Teknologi NFC Untuk Akses Pintu Masuk dan Keluar. *Jurnal Teknik Informatika*, *11*(1).

Fattah, A. 2023. Metodologi Penelitian Kualitatif. Bandung: CV. Harfa Creative

Ferdinandus, S, et al. 2023. Manajemen Risiko. Serang: PT Sada Kurnia Pustaka

Huberman, A. Michael, and Miles, Matthew B. 1994. "Data Management And Analisys Metodhs", dalam Handbook Of Qualitative Research. Norman K. Denzin dan Yvonna S. Lincoln (Ed). Thousand Oaks: Sage.

Iin, H., Pembimbing, D., Teknologi, D. M., Keahlian, B., Teknologi, M., Bisnis, F., & Manajemen, D. A. N. (2017). *Proyek Perusahaan Xyz Melalui Kombinasi*.

Kusnadi, D., and Jamal, M . 2015. "Electronic Government Pemberdayaan Pemerintahan Dan Potensi Kelurahan Pringsewu Selatan." *Jurnal TAM (Technology Acceptance Model)* 5(2):37–44.

Legowo, N., and Yoyo, J. 2022. "Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001." *Journal of System and Management Sciences* 12(3):181–99. doi: 10.33168/JSMS.2022.0310.

Pasya, A., & Wibowo, P. (2022). Analisis Peran Serta Teknologi Dalam Inovasi Pelayanan Publik Kepada Narapidana Di Era Disrupsi Pemasyarakatan Di Lembaga …. *Jurnal Pendidikan Kewarganegaraan …*, *10*(1), 462–468.

Salim, L. D., & Prasetyo, A. H. (2023). Rancangan Manajemen Risiko Dan Assesmen Risiko Pada PT Pel Berlian Pulau Mandangin Berdasarkan ISO 31000:2018. *Jurnalku*, *3*(3), 242–268.

Sandhyavitri, A., & Saputra, N. (2019). Analisis Risiko Jalan Tol Tahap Pra Konstruksi (Studi Kasus Jalan Tol Pekan Baru-Dumai). *Jurnal Teknik Sipil*, *9*(1), 1–19. https://doi.org/10.28932/jts.v9i1.1366

Sandhyavitri, A., & Young, R. J. (2004). Risk management in water supply. *People-Centred Approaches to Water and Environmental Sanitation: Proceedings of the 30th WEDC Conference*, 629–631.

Smith, C. W. J. (1990). Corporate Risk Management : Theory and Practice. *Journal De-Rivatieves*, *02*(04), 21–30.

Suyitno. (2021). Penelitian Kualitatif: Metode Penelitian Kualitatif. In *Jurnal EQUILIBRIUM* (Vol. 5, Issue January). http://belajarpsikologi.com/metode-penelitian-kualitatif/

Veronica, O., Astuti, S., Rahmadi, A. N., Sandy, D., Ilmu, J., Publik, A., Panca, U., & Raya Dringu, M. J. (2022). Efektivitas E-Government Siap Pemkot Probolinggo Dalam Meningkatkan Kinerja Pegawai Kantor Kecamatan Wonoasih. *Cetak) Journal of Innovation Research and Knowledge*, *1*(12), 1585–1590.

Undang-Undang Dasar Nomor 22 Tahun 2022 Tentang Permasyarakatan. 2022.

Peraturan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor 33 Tahun 2015 Tentang Pengamanan Pada Lembaga Pemasyarakatan dan Rumah Tahanan Negara

Peraturan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor 5 Tahun 2018 Tentang Penerapan Manajemen Risiko di Lingkungan Kementerian Hukum dan

Hak Asasi Manusia

Peraturan Menteri Hukum dan Hak Asasi Manusia Republik Indonesia Nomor 30 Tahun 2021 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia

Peraturan Penjagaan Lembaga Pemasyarakatan Direktorat Jenderal Bina Tuna Warga Departemen Kehakiman Nomor: DP.3.3/17/1 tanggal 27 Januari 1975