

Implementation of risk management in library information system at Surabaya City Library

Rudi Santoso^{1*}, Iqbal Ramadhani Mukhlis²

¹Faculty of Economics and Business, Universitas Dinamika
Jl. Raya Kedung Baruk No.98, Rungkut, Surabaya, Jawa Timur, 60298

²Faculty of Engineering and Design, Universitas Hayam Wuruk
Jl. Wonorejo Utara No.16, Rungkut, Surabaya, Jawa Timur, 60296

)* Corresponding Author, Email: rudis@dinamika.ac.id

Received: November 2022; Accepted: August 2023; Published: December 2023

Abstract

Libraries may be at risk of data security issues. The threat of data loss or data damage is prone to occur in libraries. Information technology embedded in libraries has developed Artificial Intelligence (AI) for information retrieval systems. The application of information technology in the Surabaya City Library has potential risks to data security and force majeure aspects so that need a disaster mitigation plant. This study aimed to implement information system risk management at Surabaya City Libraries as a disaster mitigation plan. The research method was descriptive qualitative. Based on the risk analysis, the recommendations for applying risk to information technology Surabaya City Library were elimination and engineering. The manifestation of these two recommendations made the data access protocol use multiple authentications to avoid data theft attempts due to infiltration, hacking, and cracking. Study results recommended a protocol for each data access. The protocol would save every change, deletion, and system login in the log history. Implementing data authentication twice per login can avoid data theft caused by the intrusion. This activity log is used for activity tracking when the system is infiltrated. The limitation of this study lies in the scope of the research object, namely the library, which has limitations on the system or application used and does not impact the wider community. Conclusion of research, the library can implement risk management strategy with elimination and engineering models through recording system login activities, which mitigate the risk of data breaches originating from insiders.

Keywords: Risk management; Library information system; Mitigation plan; Data security

Penerapan manajemen risiko sistem informasi perpustakaan di Perpustakaan Kota Surabaya

Abstrak

Perpustakaan dapat mengalami risiko masalah keamanan data. Ancaman kehilangan data atau kerusakan data rawan terjadi di perpustakaan. Teknologi informasi yang tertanam di perpustakaan telah berkembang pada Artificial Intelligence (AI) untuk sistem pencarian informasi. Penerapan teknologi informasi di Perpustakaan Kota Surabaya memiliki potensi risiko terhadap aspek keamanan data dan force majeure sehingga diperlukan rencana mitigasi bencana. Tujuan penelitian untuk mengetahui penerapan manajemen risiko sistem informasi perpustakaan di Perpustakaan Kota Surabaya sebagai bentuk rencana mitigasi bencana. Metode penelitian menggunakan deskriptif kualitatif. Berdasarkan analisis risiko, rekomendasi penerapan risiko pada teknologi informasi Perpustakaan Kota Surabaya adalah eliminasi dan rekayasa. Wujud dari kedua rekomendasi tersebut membuat protokol akses data menggunakan autentikasi ganda untuk menghindari upaya pencurian data akibat infiltrasi, hacking, dan cracking. Hasil penelitian ini merekomendasikan sebuah protokol untuk setiap akses data. Protokol akan menyimpan setiap perubahan, penghapusan, dan login sistem dalam riwayat log. Perpustakaan dalam menerapkan otentikasi data dua kali per login dapat menghindari pencurian data yang disebabkan oleh intrusi. Log aktivitas ini digunakan untuk pelacakan aktivitas saat sistem disusupi karena infiltrasi. Simpulan penelitian adalah perpustakaan dapat menerapkan strategi manajemen risiko menggunakan model eliminasi dan rekayasa berupa proses pencatatan aktivitas login sistem sebagai salah satu bentuk mitigasi risiko pembobolan data yang berasal dari orang dalam.

Kata Kunci: Manajemen resiko; Sistem informasi perpustakaan; Perencanaan mitigasi; Keamanan data

INTRODUCTION

The implementation of applications or information systems is a form of Information Technology (IT) development. The importance of implementing the information system is one form of effort to increase the productivity of the company or organization. Research conducted by Abri and Mahmoudzadeh (2015) reveals significant changes in productivity in the manufacturing industry when companies implement information systems.

The application of information systems in the manufacturing industry is straightforward to measure the level of efficiency produced. However, the conditions will differ when applying IT to non-profit entities or organizations. Non-profit organizations such as libraries are quite challenging to measure the extent of the impact or influence of IT on increasing productivity. Based on a study conducted by Hajli, Sims, and Ibragimov (2015), Polák (2017) reveals the existence of a productivity paradox in implementing IT in non-profit organizations. This is because the output of non-profit organizations is in the form of intangible products. The study by Kijek and Kijek (2019) also reaffirms that the application of IT can improve organizational performance; however, its measurement is quite tricky.

The library is a non-profit organization close to information systems and their development. Libraries are an integral part of the parent organization. However, the library is now developing into its entity (Dina & Juniarta, 2021). In the subsequent development, IT becomes a necessity in libraries (Wang, Zhong, & Li, 2022), where IT is used to help the efficiency of library administrative work. Furthermore, Kirilov and Mitev (2021) reveal that IT development is not limited

to administrative work. Information technology embedded in libraries has developed into Artificial Intelligence (AI) regarding information retrieval.

The development of artificial intelligence is also used as a demographic mapping of users. Studies conducted by Fahrizandi (2020) emphasize that the application of IT in libraries greatly assists the analysis process not only from the internal side of the library but can also provide information on changes in user behavior trends. Another finding of the benefits of using IT in libraries is based on research by Pouti and Taghva (2020) which reveals that using IT in libraries can increase the capability of library services. In other words, IT has an extraordinary role in revolutionizing library changes. Meanwhile, the library continues to develop services for its users amid change and the pandemic. Research conducted by Mahmood, Ahmad, Rehman, and Ashiq (2021) found the fact that there was a change in user behavior from conservative behavior to a more modern one. The study found a new phenomenon of increasing access to digital information by users of information portals with digital platforms. On the other hand, restrictions and regulations during the pandemic have also changed the behavior of users in seeking information. Studies conducted by Mehta and Wang (2020) reveal that the pandemic has changed the behavior of users from conventional access to digital information. This is reaffirmed by Winata, Fadelina, and Sulistyo-Basuki (2021) who found the fact that in the new normal era, users have switched to digital access rather than conventional ones.

The shift in user behavior is inseparable from the comfortable and safe feeling that users feel when carrying out

the information search process (Mansouri & Asl, 2019). These changes influence library policymakers to change conventional and digital service patterns (Twum, Yalley, Agyapong, & Ofori, 2021). Apart from speed, one of the benefits derived from the change in service pattern is accuracy. Service speed and accuracy as an excess of IT implementation are intangible outputs. So, it is also challenging to measure (Peters & Dickinson, 2020). However, implementing IT does not mean suspension because IT needs in the library have become a must.

Recent developments in IT applications in libraries have used AI to help library branding (Twum et al., 2021). The application of IT in the library has high benefits, although it is very intangible. However, on the other hand, some risks are exposed when libraries implement IT as a service tool (Brown, 2015). Some libraries implementing IT need to be literate regarding IT risks.

Several researchers, Cardoso, Moreira, and Escudero (2018) expressed the need to think and plan in as much detail as possible when libraries will migrate from conventional to digital. It is related to the level of understanding of library managers or stakeholders on the cost benefits of using IT in libraries. Another study by Schmeelk (2020) reveals that there must be a standard library digitization framework as the basis for making library Key Performance Indicators (KPIs). The indicators are used as a reference to evaluate the IT performance of the library.

In addition, based on research by Hariyanto, Ramli, and Suryanto (2021), risk mitigation is no less critical in implementing IT. Mitigating these risks is to reduce the impact of risks caused by

undesirable things such as excess IT itself. This is reinforced by Zeng (2019), which underscores the importance of providing risk mitigation as a follow-up to IT implementation.

Furthermore, this research is important because the digital era can no longer be avoided. Businesses with digital platforms are starting to consider mitigating risks from the IT they use. This is also done by libraries whose main asset is information. Research conducted by Cardoso et al., (2018) and Kirilov and Mitev (2021) reaffirmed the importance of securing data and information in the library. This confirms that risk management of library information system security is an urgent thing to do. So, the ideal library IT security risk mitigation strategy becomes an essential study.

This research focuses on applying information system risk management as a form of disaster mitigation plan. The risk that libraries most often experience is data security problems. Research conducted by Schmeelk (2020) emphasizes the need to carry out IT risk mitigation planning. Other studies related to the application of risk conducted by Qintharah (2019) and

Qintharah (2019) and Santoso and Mujayana (2021) focus on three things in the application of risk management. The three things are: 1) elimination, 2) substitution, and 3) administration. This study also provides recommendations for anticipating risks caused by force majeure in the application of IT. Especially when there is a disruption during the pandemic, IT is present as a tool that provides solutions or mediates amid the need between retaining customers and maintaining business. The study by Santoso (2022) revealed that there had been an extraordinary change in the

business map during the pandemic. These changes force business people to apply IT to maintain business during the pandemic.

Libraries present as information service providers cannot be separated from the problems of these changes. However, libraries have benefits or advantages in terms of getting to know IT in their services. At the beginning of IT development in the library, it was only used as an administrative tool. However, increasingly, library IT has developed into AI and is an inseparable part of the service elements in libraries. However, the obstacle that often occurs in libraries is that there needs to be a risk mitigation plan for implementing IT. This is exacerbated by the low literacy of the library's Human Resources (HR) related to IT. The implementation of IT in the library only relies on help from third parties.

Studies by Aremu and Saka (2014) and Enakrire and Ocholla (2017) found that most library problems are related to risk management because they buy applications from third parties and do not develop them themselves. Contrary to what has been researched by Izatri, Rohmah, and Dewi (2020), who describe that the application of risk management will be much easier to run when the library itself develops IT.

This study examined and described the application of risk management in library information systems. The review in this study focused on recommendations for library IT risk management strategies in the changing digital era. The object of this research is the Surabaya City Library Archives Agency, which has a wide range of access and users. The library is located in the middle of the city with a population of 3.3 million people, with the probability of access to the library reaching 1 million

visitors per year; the pandemic period that changed the direction of library services forced the library to optimize the use of IT to reach user services. Meanwhile, the library will also implement risk management to mitigate all possible things that will impact the continuity of library services. This study aimed to implement information system risk management at Surabaya City Libraries as a disaster mitigation plan.

RESEARCH METHODS

The qualitative descriptive approach in this study was used to analyze the dynamics of the relationship of phenomena using scientific logic. Emphasis was on a combination of library research and field research to get the most rational and up-to-date generalizations or conclusions. This study used a literature study to explore sources of information on previous research, categories, and studies related to IT risk management.

Meanwhile, field studies were carried out directly to research objects that met the criteria in this study. One of the criteria used in selecting research objects was a library that could maintain the number of visitor visits during the pandemic. In addition, the object of research must have implemented IT, not limited to the administration, but has become part of the library service in the form of an integrated library information system. This study also used a Focus Group Discussion (FGD) with the parties or stakeholders who manage the library. These parties were the head of the service, the head of the library, the library admin, and the IT department. The discussion was carried out in two directions, focusing on the risk of IT implementation in the library.

Direct interviews through FGDs were carried out at the Surabaya City Library with stakeholders involved regarding data security and risks and mitigation of handlers besides direct on-site observation by checking the feasibility

of the information system used.

This study had at least 8 (eight) stages, starting from the situation analysis of the research object to the conclusion. Figure 1 is a chart of the research stages.

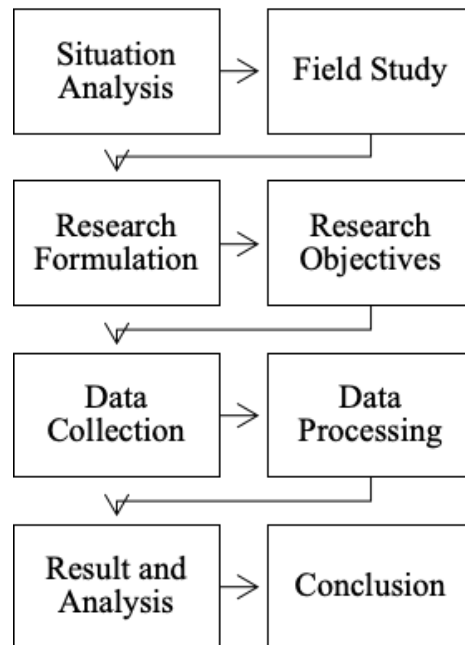


Figure 1. Research stages

Source: Santoso & Mujayana, 2021

Situation analysis is the phase of profiling the research object. Profiling is carried out to determine the potential risks that may arise. Field study is the stage to determine the scope of research, including who the object is and how broad the scope of the study will be.

Research formulation is a short statement with questions related to the research topic. In other words, the research formulation is a question that the researcher will answer using a particular method. The research objective refers to a series of questions about why the researcher should do this research. Research objectives are closely related to research novelty.

Data collection and processing is a researcher's activity of collecting

respondent data and then processing it using certain methods. The method for collecting respondent data uses a purposive sampling model. This method is used by considering that the respondents who can provide information are certain parties who have access to the library information data. The sources or respondents used were library managers such as department heads, library admins, and especially the IT department. The data in this research was taken from various library sources and then tabulated. Apart from that, qualitative data sources were also obtained from research objects and then tabulated. Data tabulation at the initial stage was carried out after verbatim transcription for further classification.

This study used a triangulation test to test the model. This test includes three activities to check the validity of the data, which include: 1) Source triangulation: This activity checks data from various research data sources to ensure the validity of the data sources. The data is then categorized to classify the same view, identify the same or different data, describe it, and then draw conclusions. 2) Engineering Triangulation: This activity checks the same source with different techniques. This activity includes in-depth interviews, observation (empirical observation), and review documents. 3) Time Triangulation: This activity checks back on data sources using the same technique but with different situations and times, repeated data checking with different times and situations to ensure the consistency of the data results obtained. The consistency of this data is needed so

that the research results are not biased. If the data obtained is different simultaneously and in a situation, then the data source cannot be used.

The informants used in this study were library staff and several information system users at the Surabaya City Library. The methods and instruments used were direct interviews and direct, on-the-spot observations to check the feasibility of the information system used. The data processing results were described in the form of a narrative for later generalization. These generalizations would be used as recommendations for decision-making.

The research stages above are continued with the application of risk management. There are at least 4 (four) stages of risk management implementation in this study; the four stages are based on figure 2.

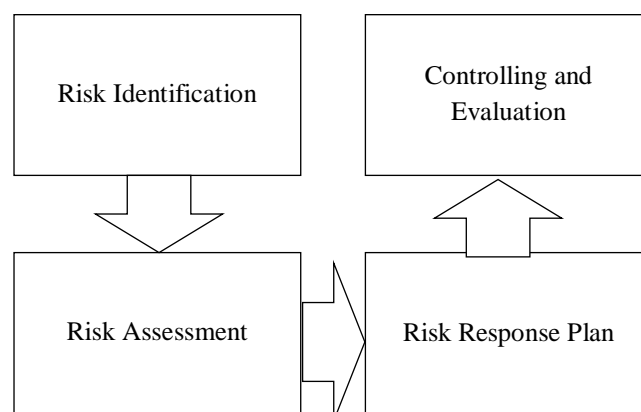


Figure 2. Risk Management Stages
Source: Santoso & Mujayana, 2021

The first stage of this research was to identify risks. Identification was done to determine all possible risks that the library would experience. The identification results were classified into level or severity, starting from very light, light, medium, heavy, and very heavy. The second stage was to carry out a risk assessment. This risk assessment

compared the impact caused by the probability level of the risk occurrence. The output of this stage was information on the type of risk impact caused in the form of qualitative information L (LOW), M (Moderate), H (High), and E (Extreme). The third stage was the response plan from the risk assessment results. At this stage, a plan was made to respond to

mitigation and risk identification results. The output of this stage would be a recommendation for the attitude to be taken. These attitudes include new service, direct action, planning risk management, and needs for stakeholder attention. The fourth stage is risk evaluation and control. This phase is a follow-up to the results of risk mitigation, divided into four elements. The four elements are elimination, substitution, engineering, and administration.

Each stage above is outlined in a table for further analysis. The results of the analysis for each stage are described in the form of a descriptive narrative. The generalization of the research is taken from the summary of all stages, which is outlined in the form of a conclusion table.

RESULTS AND DISCUSSION

The application of risk management in this study uses 5 (five) steps, including a) Determining the context of the risk, b)

Identifying Risks, c) analyzing risk, d) Evaluating Risk, and e) Implementation of Risk Management.

Determining the Risk Context: This phase aims to determine the risk targets of the Library Information System. The objectives of risk management at the Surabaya Library are a) a brief description of the potential risks that will be experienced by the City Library related to the implementation of IT; b) obtain initial input on risk management strategies to be minimized; c) advice to stakeholders on the importance of IT risk management in libraries.

Identifying Risk: At this stage, the library determines all possible risks that will occur. The identification refers to several questions about how the risk will occur. The classification used as a form of consequence consists of 5 (five) levels, namely very mild, mild, moderate, severe, and very severe. Table 1 shows the identification of library IT risks

Table 1
Risk profiling

Level	Impact	Note
1	Very light	The effect of decreasing library productivity; 5% - 10% Service is 1 - 5 minutes late from the specified SOP There are customer complaints; 1 - 5 users.
2	Light	Affect the decrease in library productivity; 10% - 15% Service is 10-15 minutes late from the specified SOP There are customer complaints; 5 - 10 users.
3	Moderate	Affects the decrease in library productivity; 15% - 20% Service is late 10-15 minutes from the specified SOP There are customer complaints; 10-15 users
4	Heavy	Affects a decrease in library productivity, 20% - 40% Service is 20 - 45 minutes late from the specified SOP There are customer complaints; 15 - 20 users
5	Very heavy	Affects library productivity decline > 40 Late service > 1 hour from the specified SOP There are customer complaints > 20 users.

Source: Data processing result, 2022

Table 1 shows that the risk is mild when the impact on the risk that arises is a decrease in performance between 5 to 10% (very light) and > 40% in very severe conditions. This decrease was caused by IT, which did not work as planned. The lightest risk had yet to have a significant impact. A decrease in productivity at a mild level of risk could still be tolerated. Libraries only needed to adjust several work SOPs to adjust the impact of risk.

Meanwhile, the risks that have begun to require attention were at a moderate level. This was because the impact began to disrupt the library's performance. One of the impacts was a decrease in performance of up to 20%. If this condition is left unchecked or is responded to late, the library's performance will continue to fall and experience a more severe risk.

In addition to the impact of decreasing the reference used was the length of service to users when compared to the SOP. The lowest range was a delay of 1 to 5 minutes. Meanwhile, the highest (severe impact) delay was more than 1

hour from the SOP. Meanwhile, the large number of complaints was also an indicator of the impact of risk. The condition was very light when the library got the number of complaints from 1 to 5. Meanwhile, in very severe conditions, user complaints >20 complaints.

The risk was too heavy when it affected the library's performance decline by more than 40%. The basic idea was that 40% was the tolerance limit because if it exceeded 40%, it would cause the library to be paralyzed due to the instability it faced. Conditions like this could lead to the paralysis of library services. If these conditions were not anticipated with various response actions, the library would not only be paralyzed entirely, but the public's trust in the library would be lost.

Library risk management also identifies possible IT risks. This is to measure and determine the position of the library quadrant when a risk occurs. The table below shows the probability of occurrence at each level of risk.

Table 2
Risk probability

Level	Probability	Note
1	Never	Once in 5 years
2	Rarely	Once a year
3	Seldom	Three times a year
4	High probability	Once a month
5	Definitely	>= Once a month

Source: Data processing result, 2022

Table 2 shows the highest level of risk probability when it occurs more than once a month. If the probability that a risk occurs more than once a month, then the library is experiencing an emergency. This is because the impact it causes is quite heavy, especially if it is severe, with a risk repetition rate of more than once a month.

It is different if the probability of occurrence is only three times in one year, then it is categorized as rare. If the risk occurs three times in one year, then it occurs once every four months. This period gives sufficient time for the library to anticipate or repair.

Meanwhile, it has never happened at the lowest level, or the probability is less than 1% every five years. These possibilities or probabilities are used to map the position of the library's quadrants so that library managers can make appropriate decisions regarding implementing risk management.

Risk analysis in the library uses a matrix model by comparing the impact of risk and the probability of risk occurrence. The two meeting points show the Library's position on the possibility of risk. The following is a matrix shown in Table 3.

Table 3
Risk impact level

Risk Freq.	Impact				
	Very light	Light	Moderate	Heavy	Worst
Definitely	M	H	H	E	E
High	M	M	H	H	E
Seldom	L	M	M	H	E
Rarely	L	M	M	H	H
Never	L	L	M	M	H

Note: L (LOW); M (Moderate); H (High); E (Extreme)

Source: Data processing result, 2022

Table 3 shows extreme impact conditions when the frequency of risk is certain, high, and rare but has a severe/very severe impact. The position of the Surabaya City Library was in the M (Middle) condition with a rare frequency of moderate impact. The most frequent IT risks the Surabaya City Library faced were data security issues and force majeure (power outages).

The case of a power outage was still something that the library could not anticipate. The library still needed a backup power source in the form of a generator set. In addition to the high investment required, the allocation of library funds was still focused on developing library collections. This power outage would be more frequent during the rainy season. Through the State Electricity Company, the Surabaya city government often turns off electricity when it rains heavily. This is to avoid short circuits caused by rainwater. The impact of this

blackout is that data access becomes paralyzed, and services cannot be carried out because the application requires a source of electrical energy. Meanwhile, the library still needs to be equipped with a generator set as backup power. So, when there is a power outage, the library runs the risk of data loss. In addition to data loss, sudden power surges will cause electronic devices to malfunction.

The potential for damage to electronic equipment will be a severe risk and harm to the library if the risk occurs more often. In addition to the blackout factor, the library also has the potential to experience illegal access by library users.

However, illegal data access to the library is rare, with moderate impact. Infiltration, phishing, or cracking of library data is rare. Even if the probability exists, it is only once a year. IT admins can quickly anticipate this, so the impact is not too worrying.

Risk mitigation is based on the position of the matrix above and then re-analyzed to make a decision. Decision-making on the results of the analysis of the

table above refers to the representation of the matrix results. The following is a representation of each risk level, which is shown in table 4.

Table 4
Recommendation

Level	Recommendation
Low	New service SOP
Middle	Direct action
High	Planning risk management
Extreme	Need attention stakeholder

Source: Data processing result, 2022

Based on the recommendation in table 4, the position of the IT risk matrix of the Surabaya City Library is in the middle position. The follow-up recommendation in this position is direct action. As explained in the previous paragraph, data infiltration is the most likely risk in such a library. This event has a probability of occurring only once a year. The impact is still light, so the mitigation carried out by the library is to take direct action when the risk occurs.

Apart from data infiltration, the most significant potential risk impact is when a power outage occurs. Even though the frequency of power outages occurs once a year, the impact is quite severe. Besides being able to paralyze library services, library digital data also has the potential to be damaged. The damage is caused by malware due to a sudden power surge.

Evaluating Risk: This stage is a follow-up to risk mitigation. The recommendation reference chart is as follows in figure 3.

RELIABILITY	Eliminate	PROTECTION
	Substitution	
	Engineering	
	Administration	

Figure 3. Risk control

Source: Santoso & Mujayana, 2021

Based on figure 3, there are four types of risk control evaluation, namely elimination, substitution, engineering, and administration. The four types of recommendations depend on the impact of each risk. The following is an elaboration of risk control recommendations for the Surabaya city library:

Eliminate; This recommendation directs to avoid the risks that will arise immediately. The source of the risk of implementing IT in the Surabaya City Library is related to data security. This study recommends data access protocols in every service process to avoid data theft, infiltration, hacking, and cracking. This protocol is used as a basis or reference

for providing services related to important library data.

The access protocol is also used as a Standard Operating Procedure for each data access activity. This is very important to avoid the risk of infiltration from unwanted parties. The use of Hypertext Transfer Protocol (HTTP) in the Surabaya city library information system is no longer sufficient to avoid data infiltration. So, the use of Hypertext Transfer Protocol Secure (HTTPS) is the minimum choice to protect library data.

The HTTPS protocol has higher security compared to HTTP. As the name implies, HTTPS is a more secure protocol. This protocol will protect the integrity, confidentiality, and data security between site users and computers. So, it is better to use HTTPS protocol, not just HTTP, to protect library user data. The recommendation for using the HTTPS protocol also refers to research results from Glăvan, Răcuciu, Moinescu, and Eftimie (2020) and Madasu (2015), which reveal the fact that the HTTPS protocol is more widely used as a standard protocol to protect the confidentiality of internet site user data.

Substitution: One of the risks the Surabaya City Library faces is the systematic risk as a force majeure. The risk is when the electricity goes out, which can paralyze digital-based services. The recommendation of this research is to substitute for backup electrical power in the form of a Generator Set (Genset). The generator will be useful to replace electric power if there is a power outage at any time.

Using a generator set as a backup power source would make more sense than just waiting for the power source to turn back on. It is time for the library to

consider investing in a generator set as a backup source of electrical energy. Of course, the generator set investment must also be considered, and the resulting cost benefits must be calculated. The cost-benefit analysis of the generator set investment can use the time value of money and Return on Investment (RoI) models. Accurate calculation and analysis of these investments will make library performance more efficient and effective. The recommendation to use a generator set as a backup energy source refers to research by Costa and Villalva (2020), and Vempere, Jasevics, Zemite, and Vempers (2021), which reveals that the use of alternative energy as a backup source of electricity can help efficiency and avoid the systematic risk of scarcity of electrical energy.

The model for calculating the time value of money from the generator set investment refers to the Future Value formula. The calculation is multiplying the present value by the interest factor $(1+r)$ by the power of n . The number 1 is the given unit, while r is the set annual rate or appreciation value. Meanwhile, n is the compounding period of the investment.

Calculating RoI from generator set investment using the RoI calculation method. The calculation is the total income minus the initial capital, then divided by the initial capital. Because the library is a non-profit organization, the calculation refers to the output of intangible service performance and then makes a scale to be nosed quantitatively. The results are then compared with the conditions before applying the generator set. The resulting output is in the form of qualitative recommendations, no longer a quantitative number. This is because the library is a

non-profit organization with a core service business.

Engineering, infiltration, hacking, and cracking are still the scourge of IT implementation risks. So, this study recommends a protocol for every data access. The protocol will save every change, deletion, and system login in a log history. In addition, implementing two times data authentication per login can avoid data theft caused by infiltration.

Every activity related to the information system will be recorded in a history log. The activity record is used as activity tracking material when the system experiences problems due to infiltration. Even though the library information system already uses the HTTPS protocol, there is still the potential for data breaches. In this condition, it is usually done by an insider who has login access to the system. So, recording system login activities is a form of mitigating the risk of data breaches from insiders.

Administration; One of the obstacles that are often faced by library services is service procedures. This can be trimmed by implementing IT in every library business process. The application of a library information system is one of the most efficient alternatives to cut service procedures. The application of IT to library information systems also avoids human error in every service. This human error is related to the level of work endurance of library staff. This administrative recommendation supports research conducted by Gotovac, Zelenika, Marušić, and Božić-štulić (2020) and Sharma and Rawal (2021), which reveals that the application of IT in every service will minimize the risk of human error. Especially if the service industry that. Given requires a high level of precision,

the application of IT in the service sector is one of the alternative recommendations for risk mitigation.

Implementation of Risk Management: The application of risk management at the Surabaya City Library refers to the recommendation table for the matrix representation table. Surabaya City Library's IT position is in direct action. So, the most rational application that can be done in this case is elimination and engineering. Applying this technique of elimination and engineering refers to the probability or possibility of a risk occurring to the security of library data. Implementing protocols in every library service business process can eliminate library data theft. Access to essential library data must go through two authentications to ensure that access does not originate from infiltration. Engineering begins with building business process flows related to the input process output. The flow is then translated into additional applications as an inseparable part of the IT library.

Some risks are inevitable, such as business failure, where the risk is a risk that has a probability of 50 percent. The problem is that we need to know when this risk will befall our business unit. In general, the risks we usually face are the risk of business loss, force majeure, and technical risks so that services cannot be provided. There are four ways to manage library risk: Risk Awareness, Assess, Treat, and Monitor.

Being aware of risk is the beginning of all these processes. A company leader must be highly aware of the risks of the company he leads. This awareness is related to the company leader's complete understanding that risks must be appropriately managed. This risk

awareness continues up to the assessment of the level of risk to be managed.

Meanwhile, the risk assessment is adjusted to the nature and characteristics of the risk itself. For example, when assessing the risk of a building fire, one can use a physical audit in one's assessment. The same is true when assessing business risk. Business risk requires more detailed research and analysis. The risks that occurred in the past are used as the basis for analysis to find out the causes. This cause can occur due to poor performance, management negligence, or other reasons.

Several assessment techniques are commonly used by companies in assessing risk. However, the most commonly used are audits and measurements. Assessment stage measurements allow the corporate president to analyze and make decisions. After this stage is completed, the company will determine the priority scale of corporate steps. So that corporations can identify which hazards or indicators can provide more significant risk.

The next step is the treatment of those risks. Risk treatment involves avoiding, minimizing, spreading, and accepting. Avoided risks can have a significant impact on a company/corporation. Risks can be minimized if these risks can be reduced by increasing controls. Risk can also be transferred or diversified. The usual practice is to do outsourcing, hedging, and insurance. The final step in the risk management stage is monitoring. A repair audit accompanies this step to ensure operational procedures are correctly carried out.

The next step is to provide feedback on the risk analysis results. This response is the determination of the company's

attitude toward the risks that will be experienced. Some of the responses or determination of attitudes from the results of the analysis are as follows:

Risk avoidance: This attitude is to stop all activities that can pose a potential risk. In other words, the company tries to avoid all activities that are unprofitable and potentially risky. Risk sharing or transfer action is usually called hedging or outsourcing. The company will transfer the risk to other parties using specific mutually beneficial schemes.

Risk reduction: This action is usually used by companies that do not avoid risk and will still face it. One way is to reduce the impact caused. Implementing internal controls within the company reduces the impact caused by this. **Risk acceptance:** This action is almost the same as point 3, but in this phase, the company takes risks without taking any action to reduce or overcome the impact it causes.

CONCLUSION

The Surabaya City Library needs to implement risk mitigation in IT through elimination and engineering. This research provides recommendations for mitigating the risks of implementing IT in libraries, both caused by force majeure and interference from outside the library. The results of the study provide recommendations for eliminating all potential risks from outside the library, such as infiltration, hacking and data hacking. The limitations of this research lie in the research object, where the data from the research object is still small compared to IT data on public services. Recommendations for further research are this risk management model or application that can be used for service organizations with more extensive data, for example,

Information Technology applications in population service agencies whose risk potential is more significant than library entities.

REFERENCES

- Abri, A. G., & Mahmoudzadeh, M. (2015). Impact of information technology on productivity and efficiency in Iranian manufacturing industries. *Journal of Industrial Engineering International*, 11(1), 143–157. <https://doi.org/10.1007/s40092-014-0095-1>
- Aremu, M. A., & Saka, H. T. (2014). The impact of information technology on library management: A marketing perspective. *Arabian Journal of Business and Management Review (OMAN Chapter)*, 4(4), 1–10. <https://doi.org/10.12816/0019058>
- Brown, M. M. (2015). Revisiting the IT productivity paradox. *The American Review of Public Administration*, 45(5), 565–583. <https://doi.org/10.1177/0275074014523102>
- Cardoso, A., Moreira, F., & Escudero, D. F. (2018). Information technology infrastructure library and the migration to cloud computing. *Universal Access in the Information Society*, 17(3), 503–515. <https://doi.org/10.1007/s10209-017-0559-3>
- Costa, T. S., & Villalva, M. G. (2020). Technical evaluation of a PV-Diesel Hybrid system with energy storage: Case study in The Tapajós-Arapiuns Extractive Reserve, Amazon, Brazil. *Energies*, 13(11), 1–22. <https://doi.org/10.3390/en13112969>
- Dina, N. Z., & Juniarta, N. (2021). Research on application of information technology for library information service. *Library Philosophy and Practice*, 1(1), 1–12. <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=12441&context=libphilprac>
- Enakrire, R. T., & Ocholla, D. N. (2017). Information and communication technologies for knowledge management in academic libraries in Nigeria and South Africa. *South African Journal of Information Management*, 19(1), 1–9. <https://doi.org/10.4102/sajim.v19i1.750>
- Fahrizandi. (2020). Pemanfaatan teknologi informasi di perpustakaan. *Tik Ilmieu: Jurnal Ilmu Perpustakaan Dan Informasi*, 4(1), 63–75. <https://doi.org/10.29240/tik.v4i1.1160>
- Glăvan, D., Răcuciu, C., Moinescu, R., & Eftimie, S. (2020). Man in the middle attack on HTTPS protocol. *Scientific Bulletin of Naval Academy*, 23(1), 199–201. <https://doi.org/10.21279/1454-864X-20-I1-026>
- Gotovac, S., Zelenika, D., Marušić, Ž., & Božić-štulić, D. (2020). Visual-based person detection for Search-and-Rescue with UAS: Humans vs. machine learning algorithm. *Remote Sensing*, 12(20), 1–25. <https://doi.org/10.3390/rs12203295>
- Hajli, M., Sims, J. M., & Ibragimov, V. (2015). Information Technology (IT) productivity paradox in the 21st century. *International Journal of Productivity and Performance Management*, 64(4), 457–478. <https://doi.org/10.1108/IJPPM-12-2012-0129>
- Hariyanto, B., Ramli, K., & Suryanto, Y. (2021). Risk management system for

- operational services in data center : DC Papa Oscar Cikeas case study. 2021 *International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*, 118-123.
<https://doi.org/10.1109/ICAICST53116.2021.9497845>
- Izatri, D. I., Rohmah, N. I., & Dewi, R. S. (2020). Identifikasi risiko pada perpustakaan daerah Gresik dengan NIST SP 800-30. *JURIKOM: Jurnal Riset Komputer*, 7(1), 50.
<https://doi.org/10.30865/jurikom.v7i1.1756>
- Kijek, T., & Kijek, A. (2019). Is innovation the key to solving the productivity paradox? *Journal of Innovation & Knowledge*, 4(4), 219-225.
<https://doi.org/10.1016/j.jik.2017.12.010>
- Kirilov, L., & Mitev, Y. (2021). An approach for implementing the information technology infrastructure library. *Comptes Rendus de l'Academie Bulgare Des Sciences*.
<https://doi.org/10.7546/CRABS.2021.05.11>
- Madasu, V. K. (2015). Web authentication and authorization and role of HTTP, HTTPS protocol in networking. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, 2(3), 381-383.
<https://www.jmest.org/wp-content/uploads/JMESTN42350525.pdf>
- Mahmood, K., Ahmad, S., Rehman, S. U., & Ashiq, M. (2021). Evaluating library service quality of college libraries: The perspective of a developing country. *Sustainability*, 13(5), 1-13.
<https://doi.org/10.3390/su13052989>
- Mansouri, A., & Asl, N. S. (2019). Assessing mobile application components in providing library services. *The Electronic Library*, 37(1), 49-66. <https://doi.org/10.1108/EL-10-2018-0204>
- Mehta, D., & Wang, X. (2020). COVID-19 and digital library services: A case study of a university library. *Digital Library Perspectives*, 36(4), 351-363.
<https://doi.org/10.1108/DLP-05-2020-0030>
- Peters, T., & Dickinson, T. E. (2020). A history of the distance library services conference. *Journal of Library & Information Services in Distance Learning*, 14(2), 96-109.
<https://doi.org/10.1080/1533290X.2020.1809600>
- Polák, P. (2017). The productivity paradox: A meta-analysis. *Information Economics and Policy*, 38(1), 38-54.
<https://doi.org/10.1016/j.infoecopol.2016.11.003>
- Pouti, N., & Taghva, M. R. (2020). Determining organizational maturity of information technology with information technology and business alignment approach by capability maturity model integration and best practices of information technology infrastructure library: Case study Kermanshah E. *Iranian Journal of Information Processing and Management*, 35(2), 519-552.
https://jipm.irandoc.ac.ir/article_699590_79a3d7cc0cfbcd6e79e258241681b194.pdf?lang=en
- Qintharah, Y. N. (2019). Perancangan penerapan manajemen risiko. *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi*, 10(1), 67-86.
<https://doi.org/10.33558/jrak.v10i1.1645>

- Santoso, R., & Mujayana, M. (2021). Penerapan manajemen risiko umkm madu di kecamatan badas kabupaten kediri di tengah pandemi Covid-19. *Jurnal Nusantara Aplikasi Manajemen Bisnis*, 6(1), 74-85. <https://ojs.unpkediri.ac.id/index.php/manajemen/article/view/15643/2005>
- Santoso, R. (2022). Disrupsi pandemi dan strategi pemulihan industri kreatif. *Jurnal Manajemen Dan Kewirausahaan*, 7(1), 48-58. <https://ejournal.uniska-kediri.ac.id/index.php/ManajemenKewirausahaan/article/view/2101/1453>
- Schmeelk, S. (2020). Creating a standardized risk assessment framework library for healthcare information technology. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 3881-3890. <https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/25a313a2-9ca6-4df1-913c-26fe0dc79b98/content>
- Sharma, S., & Rawal, Y. S. (2021). The possibilities of artificial intelligence in the hotel industry. *Proceedings of First Global Conference on Artificial Intelligence and Applications (GCAIA 2020)*, 695-702. https://doi.org/10.1007/978-981-33-4604-8_53
- Twum, K. K., Yalley, A. A., Agyapong, G. K.-Q., & Ofori, D. (2021). The influence of public university library service quality and library brand image on user loyalty. *International Review on Public and Nonprofit Marketing*, 18(2), 207-227. <https://doi.org/10.1007/s12208-020-00269-w>
- Vempere, L., Jasevics, A., Zemite, L., & Vempers, G. (2021). Methodology for investment evaluation in electricity generation modules according to the requirements of the European Union. *Latvian Journal of Physics and Technical Sciences*, 58(3), 15-31. <https://doi.org/10.2478/lpts-2021-0014>
- Wang, D., Zhong, D., & Li, L. (2022). A comprehensive study of the role of cloud computing on the Information Technology Infrastructure Library (ITIL) processes. *Library Hi Tech*, 40(6), 1954-1975. <https://doi.org/10.1108/LHT-01-2021-0031>
- Winata, A. P., Fadelina, R., & S.-B. (2021). New normal and library services in Indonesia: A case study of university libraries. *Digital Library Perspectives*, 37(1), 77-84. <https://doi.org/10.1108/DLP-07-2020-0059>
- Zeng, W. (2019). A methodology for cost-benefit analysis of information security technologies. *Concurrency and Computation: Practice and Experience*, 31(7), 1-12. <https://doi.org/10.1002/cpe.5004>