Jurnal Borneo Administrator
Volume 17 (3) 2021: 291-304
P-ISSN: 1858-0300, E-ISSN: 2407-6767
DOI: 10.24258/jba. jba.v17i3.927
Accredited by Kemenristek/BRIN No. 148/M/KPT/2020

ARTICLE

Holistic Approach in Risk and Security Management on Public Information

Yudie Aprianto

Doctoral Program, Department of Communication Science, Faculty of Social and Political Sciences, Universitas Gadjah Mada, Yogyakarta, Indonesia.

How to cite: Aprianto, Y. (2021). Holistic Approach in Risk and Security Management on Public Information. *Jurnal Borneo Administrator*, *17* (3), 291–304. Doi: https://doi.org/10.24258/jba.v17i3.927

Article History
Received: 09 July 2021
Accepted: 15 November 2021

Keywords:
Public Information, Information Security, Information Management, Information Risk

ABSTRACT
Public information is one of the government's efforts to provide public information regarding their performance and activities. However, even some regulations guide them, practice in public information management has not been optimal considering the information risks and threats, such as disclosing inappropriate information. For this reason, the literature study seeks to explore some efforts that can be made in information management, especially in Indonesia. This qualitative study tries to categorize and describe the management of public information in risk management and public information security in terms of technological management, process management, and human resource management. Technological management is expected to have an information system capable of providing a sense of security from threats, both malware and in building an effective system. Process management includes procedures, auditing, and a holistic approach to realizing effective public information management. Finally, human resource management emphasizes the importance of improving the quality of agents through training and leadership to act not only as a leader but also as a navigator and a translator of public information management. This study proposes a conceptual model based on those themes to minimize the effects of risks and threats on public information. Limitations and suggestions for future research are also discussed.

A. INTRODUCTION

Information has an essential role in everyday life. Through information, we can meet our needs for all information related to interests that are being sought. Similarly, in the organization's context, information also plays an essential role in the sustainability of an organization. Kaye (1995:6) stated that through information, organizations could improve the quality of decision making, the efficiency of business processes, and provide needs in competing with others. An organization that pays attention to the environment and information, both related to its business and other information (information on conditions from various aspects such as politics and culture), in formulating and monitoring its business strategy, can provide stability in its business operations (Kaye, 1995).

Similarly, various forms and types of information are also needed in carrying out organizational processes in government organizations. For example, a government institution in education seeks data and information from schools in a particular area to determine policies in improving the quality of schools in the area. However, government institutions are not only

* Corresponding Author
Email : yudie.aprianto@gmail.com

actively seeking information. They also need to process, organize, and convey their information to the public. For example, a public organization in disaster management aims to provide information about potential disasters in a certain area after conducting research. Providing information like this to the public can help the community in disaster preparedness and the government policy-making process.

However, the policy itself is not necessarily able to effectively impact public information management. Regulations related to public information, such as in the UK, Perri et al. (2010) showed an anxiety from the risk of large-scale data loss that has undermined confidence in public services towards confidentiality. This is due to the inadequacy of the current emphasis on formal regulatory instruments to guide public services in addressing this poses a dilemma (Perri et al., 2010). They suggest the need to develop confidence and skills in implementing professional assessments of public information and demonstrate the value of heuristic frameworks drawn from risk analysis and management.

The study of public information risk management has not been widely studied. This can be seen from the search results for articles and proceedings within 1975-2021 using the Vosviewer application. It shows that public information has a reasonably small intensity. That is related to the implications of public perception of information (Lepesteur et al., 2008) and communication of public information that can increase public engagement (Cochrane et al., 2011), but not directly with risk management of the public information (Figure 1).

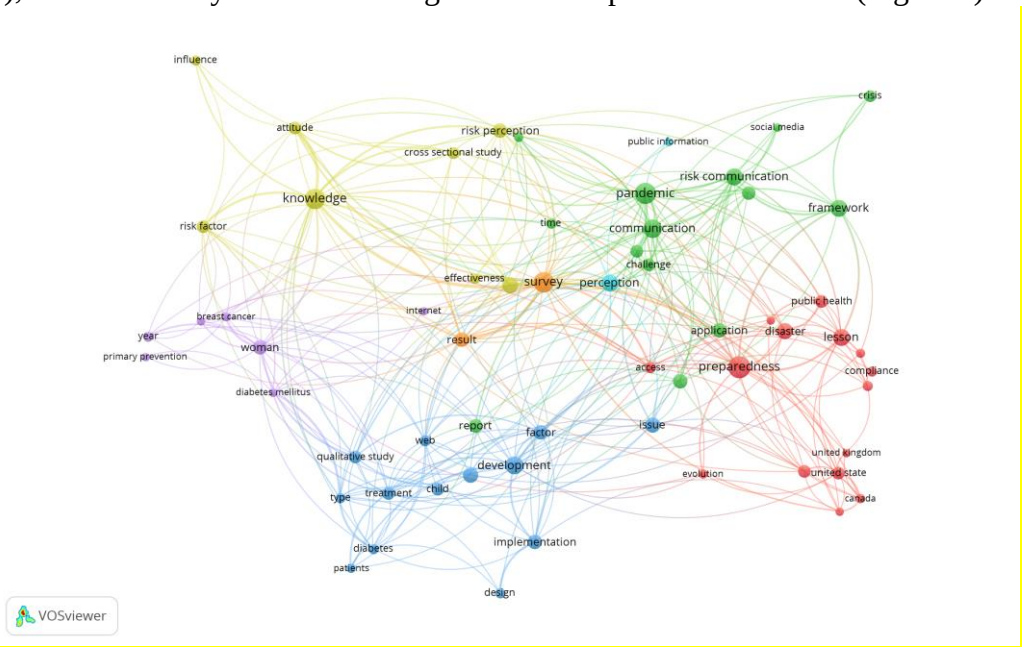

Figure 1. Map of the Emergence of Keywords in Public Information Risk Management Research

Public information is still being studied merely as use of data (Campomizzi et al., 2012; Wieder et al., 2018) . It is, therefore, necessary to discuss risk management and ethics in public information (Bieri, 1994), given the potential for control of data that has the potential to harm the public (Avery & Lariscy, 2011). Less effective risk management can result in material and non-material such as declining reputation and public trust in the organization. On the one hand, public information becomes a thing that must be conveyed to the public. However, public information has potential risks and security elements that are considered. Thus, public information management becomes an important thing to do considering the existing threat to the possibility of less effective information management. Therefore, comprehensive risk mitigation efforts are essential to be carried out by organizations (Irianto & Ispriyarso, 2016)

to create holistic management of public information and overcome conflicts of interest in public information disclosure. In addition, search results show public information studies and risk management are still dominated by reflections from the west, such as the United Kingdom (Campomizzi et al., 2012), the United States (Sexton, 2013), and Canada (Dunn et al., 2014).

For that reason, this paper was written to explore the existing literature in providing a more comprehensive description of the risks and security of public information and provide an overview of public information management in Indonesia to enrich the study amid many studies from the west. In addition, exploration is also carried out on various activities to manage risks and information security that need to be done to describe the effective management of public information.

B. LITERATURE REVIEW

Conceptualization of Public Information in Information Management

According to Bouhadana (2016:2), public information is produced, held, and received by government institutions. So that information from a public institution can be viewed as public information. According to Law No. 14 of 2008 on Public Information Disclosure (after this referred to as *KIP* Law), public information is defined as "information generated, stored, managed, transmitted, and/or received by a public agency related to the organizers and administration of the state and/or the organizers and the administration of other public agency by this law as well as other information related to the public interest" (*KIP* Law, 2008). In the KIP Law, public information is data and information generated or related to the use of budgets both from the government and grants from home or abroad in government and non-governmental institutions, including information that needs to be known by the public. However, in the *KIP* Law, it is also mentioned about the exclusion of information that is not included in public information, namely confidential information in accordance with regulations, fairness, and public interest. Such excluded information is based on a process of testing the consequences of the possibilities arising if it is provided to the public and has considered greater protection of interest than opening it or otherwise be the case.

In more detail, Government Regulation (in the future as *PP*) No.61 of 2010 explains that excluded information is information that could potentially hinder the process of law enforcement (identity of the informant, whistle blower, witness, or victim), limited by the provisions of other laws. Then regulations (trade secrets, patents, and prohibition of monopoly practices) which can endanger the country's defence and security (documents related to the country's defence and security system). It can harm national economic resilience (exchange rate change plans), can damage the interests of foreign relations (diplomatic correspondence between countries), and can uncover personal secrets (a person's history of condition and treatment). Furthermore, in the PP, it is also mentioned if the excluded information has expired, the exclusion period then becomes public information that the public information applicant can access with the determination of the Information and Documentation Management Officer (in the future referred to as *PPID*) of the institution.

Disclosure of Public Information as An Important Aspect of Public Information Management

There are two main concepts in the openness of public information, namely openness and access to *information*. In this regard, transparency and access to information are understood as activities that can or should be taken by public authorities in support of public transparency. Boserup et al. (2005) explain that such activities include (1) the provision of access to the initiative of public bodies themselves to the information they hold, (2) granting access to requests for information they hold, (3) public engagement through hearings, meetings and open

campaigns, and (4) public engagement in the formulation and implementation of policies through participation in relevant committees, councils, and other parties.

In the context of Indonesia, the openness of public information contained in the KIP Law is defined as "... means in optimizing public supervision of the implementation of the state and other Public Entities and everything that results in the public interest" (KIP Law, 2008:1). Public information disclosure is part of a democracy where freedom and human rights in obtaining public information and this mandate are contained in the KIP Law. However, the information released can not only have a positive impact. Information poorly managed information can risk either the opening up of confidential information, modification of inappropriate information, or loss of data (Blakley et al., 2001). For example, Rahmanto (2021) explained the potential risks of information security from land data in Indonesia. There are contradictions in the openness of public information through the KIP Law and the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (in the future referred to as *ATR/BPN*) in maintaining data confidentiality. The management aggravates this within the organization, which still has available and limited information arrangements. In addition, the results of studies from Irianto and Ispriyarso (2016) also showed a conflict between the KIP Law and ethical principles in banking, especially related to the limitations of information provision.

Efforts to look at public information management of regulatory approaches can also be seen in the Bouhadana study (2016), which looked at public information problems in terms of international regulations. There are also country-specific ones, such as studies on access to public information in Italy (Galetta, 2018), America (Vaughn & Messitte, 2018), and Sweden (Jonason, 2018). On the other hand, public information management is more likely to be studied with specific approaches, such as the Sundgren study (2012), which uses information technology approaches in public information management. It is even less comprehensive because he considers fewer organizational aspects and emphasizes the technological aspect (Sundgren, 2012).

Meanwhile, the large gap between policy, planning, and realization can complicate the implementation of public information disclosure (Widodo, 2013). Furthermore, bureaucracy in public organizations tends to maintain the status quo rather than developing transparency and public capacity to access needed information (Linden, 1999). In support of this policy, information technology has provided many new opportunities to exchange data, information, and knowledge without significant constraints regarding distance, time and place. This makes the government can use information technology optimally in its governance.

In its implementation, Morris and Shin (2002) stated that public information disclosure has attributes that make it a double-edged public policy instrument that, while very effective in influencing the actions of public entities to be transparent, there is still the possibility of extreme action against public information, and therefore unexercised public information or disclosure of misinformation can cause major harm.

However, the study still focuses on formulating regulations that support public information disclosure and emphasizes less on how to build systems that can comprehensively manage public information effectively. Therefore, in creating transparency, information openness has potential risks that need to be considered and requires a comprehensive approach to managing public information risks and security.

Conceptualization of Public Information Security and Risk

Whitman and Mattord (2011) define information security as information protection and other critical elements that include the systems and software used, storage, and transmission of information. In concept, Von Solms and Van Niekerk (2013) explain that information security is seen not only as a product or a technology but as a process. Information protection is related

to technical problems in information systems and networks and involves various associated resources. In addition, Von Solms and Van Niekerk (2013) also disclose properties or characteristics that secure information should have, i.e., confidentiality, integrity, and availability of information, but may include other additional parts.

In more detail, Peltier (2013) mentions that eight elements in information security include (1) it must support business objectives; (2) there is the integration between the role of loyalty and the role of protecting the organization; (3) it has an effective cost (4) it is explicit in determining responsibility and accountability; (5) the owner of the security system is responsible for the security of information outside the organization; (6) it uses a comprehensive and integrated approach; (7) it conducts periodic assessments or evaluations; and (8) it considers aspects of organizational culture. Information security requires a holistic strategy and a high commitment to protecting the organization's resources.

From that conception, it can be known that information is always at risk, and information security is basically about risk management to ward off threats to information systems and the data they contain (White, 2015). Information risk is the identification of the likelihood of an event that will reduce the value of information under the conditions that will occur (Blakley et al., 2001). For example, if an organization's information is at risk, we rely on technology to maintain information security. Information security is necessary because the technology applied to information can pose a risk.

Rational Approach to Security and Risk of Public Information

According to Njenga and Brown (2012), generally, the views in risk management and information security use a rational approach that emphasizes the mechanisms of practitioners that rely on standardized formal methods and criteria. However, it has disadvantages where predictability is very low in managing information with a lack of reliable empirical data regarding the frequency and amount of losses caused by information security compromises and scarcity of different types of information security compromises (Njenga & Brown, 2012). Thus, there is a duality in looking at risk and information security, namely, overcoming threats or risks that can be predicted and unpredicted (Spagnoletti & Resca, 2008). It is also conveyed by, who argues that the probability of information security is often determined by perception and heuristics, which can ultimately lead to inaccurate risk determination when this method is used. For that reason, careful consideration should be taken when using these, or other models, to determine an organization's security risks (Taylor, 2015).

Holistic Approach: Alternative Models of Public Information Security and Risk Management

On the other hand, current trends, approaches in information security and risk have used approaches from social theories (Njenga & Brown, 2012). This is also in line with the opinion of Singh et al. (2013), which illustrates that in the beginning, information security management was treated as a technical problem, and most of the attention was paid to technological solutions. Nevertheless, as it progresses, Siponen et al. (2014) state that information security issues should also be considered in the context of management. The illustration shows that information has risks, and management in information is necessary not only to protect the information itself but also to protect and support the organization. Consequently, the necessary approach includes a rational view of information and all aspects related to information is an important part of managing information or emphasizing a more comprehensive approach to risk management and public information security, both predictable and unpredictable ones.

C. METHOD

The study was conducted with a qualitative approach to synthesize existing literature to understand a more holistic approach to risk management and security of public information. Literature search in the form of scientific journals, books, reports, related news articles, and publications in the media with the keywords "risk information" and "public information" using the Publish or Perish application with Google Scholar database and indexed by Scopus, and Vosviewer. Themes appeared from the search and then grouped the articles into several themes (Strauss & Corbin, 1998). Existing themes were then analyzed in narrative form to describe the theme in detail through subtheme (Creswell & Creswell, 2018).

D. RESULT AND DISCUSSION

From the study of related literature, several major themes need to be understood related to the management of public information security which includes: risk and security of public information (insecurity of personal information and public information, threats to information systems, and accountability of public information); risk management and public information security which consists of technology management, process (information auditing and procedures); and human resource management through effective training and leadership.

Risks and Security of Public Information

Public information disclosure is seen as the only thing that can risk public information. White (2015) states that information is always at risk and information security is essentially about risk management to ward off threats to information systems and the data they contain. For example, Lee (2019) explained the risks of information about the issue of nuclear power that tends to be viewed negatively. Furthermore, Lee and Kwon (2019) stated that information risks related to decisions, actions, and policies are used to control and manage risks between that group. More specifically, here are some risks associated with public information.

1. The Vulnerability of Personal Information and Public Information

Public information also has a strong connection with information that is private. Generally, all public information is spread out among various databases that are not integrated, and management seeks to integrate existing information. For some public entities, there is a need to integrate client information in one place or system, such as defence agencies, foreign countries, prosecutors, and police. However, Switzerland (2007) allows sensitive information that every internal worker easily access through a single-stop shopping system and potential privacy violations and information leaks from the amount of information available. Because more and more management information services are outsourced, however, it still can increase the risk of information leakage due to the large number of people who have access but reduce the access of government leaders to monitor them directly.

The ambiguity of personal and institutional data is also present in the issue of disputes over the openness of public information. A court decision of the Central Information Commission stated that applicants for information (public) could obtain information on government employees in the form of salary details, employee appointment decrees, and details of employee work attendance (Central Information Commission, 2019). The KIP Law Article 6 states that information related to personal rights is public information that is excluded. Therefore, this indicates the risk of personal information being disclosed to the public due to public agency employees.

2. Threats to Information Systems

Advances in technology and information systems in public information management have benefited the efficiency and effectiveness of public information management. Almost all

business processes carried out by public organizations are electronic transactions, or at least in their internal systems. However, this is inseparable from security threats and risks. White (2015) mentions the existence of malware or software harmful to information systems that can impact data loss, data theft, and damage to the entire system. In addition, the threat of the system is also vulnerable to survivors or hackers. To that end, information security becomes essential in the context of information systems and computing. Furthermore, Sundgren (2012) argues that emphasising technological aspects in public information management is insufficient and optimizes organizational aspects (Sundgren, 2012).

3. Accountability of Public Information

Threats to information security and their risks have a major impact, measurable and unmeasurable. White (2015) describes the risks from information security as a serious issue because reports of failure to handle information risk resulted in considerable financial and operational losses.

In addition to measurable losses, risk and information security are also intangible. The issue of public information affordability in an article written by Fakih and Lawati (2019) exposes the risks in the affordability of public information of an institution. They emphasize the importance of information systems such as websites that provide information related to public services. This will reduce the complexity and difficulty of information needed by the public in getting public services of an organization.

In addition, there are risks in the delivery or translation of information between the organization and the public from negative public perception, ineffective and persuasive information, lack of mutual information deliberation from various parties (Lee, 2019). The problems shown in information risk and security are complex, related to physical resources, information, and humans. Thus, in public information management decision-making, management commitment needs to focus on policy decision-making about the desired balance between efficiency, usually promoted by making complete information accessible to employees, and information security.

Risk Management and Public Information Security

Information that is considerably owned by public entities encourages them to do information management. Determination in choosing how public information is managed also shows that expertise in understanding information and how information is delivered is important to have. Meijer and Thaens (2009) explain some opportunities for government agencies to manage their information. First, hold information for agencies so that information is not actively circulated to the public. Second, present information on government websites to make this information available to citizens and commercial actors. Third, sell information to information intermediaries who offer information on the website to citizens. Fourth, provide information to information intermediaries who offer information on the website to citizens. In general, government agencies are forced to choose one of the options of supplying or refraining from publishing information when no reliable information intermediary is available.

The institutional context makes those choices, and, at the same time, these institutional contexts may change through selection (Orlikowski, 1992). The regulation of certain information can influence informal rules that guide the behaviour of actors in a sector. These arrangements can even affect the legal and political context when new rules are needed, or political relations change. Specific information management options are studied as rational choices and as a process of institutional change. This is in line with Kim dan Kim (2020) that the relationship between the implementation of information technology and effectiveness is inseparable. To that end, this paper then offers a management approach in managing public

information that is interrelated in terms of technology, processes, and human resource management.

1. Technology Management

In providing public information, containers and channels alone are not enough. Several things need to be facilitated to run public information management effectively. According to White (2015), an established information system is a system that is resistant to malicious software such as viruses, spyware, adware, spam, and phishing. The effects of malware can range from those that disrupt the system and employee performance, such as the sheer number of unwanted spam emails, to highly damaging results, such as losses. Spam is becoming a problem because of the sheer amount of resources requested and because it now serves as a means for other types of attacks. Phishing can lead to identity theft and loss of sensitive information; This can easily result in reduced trust and, therefore, the use of government electronic services, thereby reducing the efficiency offered by such services.

In addition to resistance to malware, technology in public management is also expected to provide a comprehensive picture of environmental conditions. For example, He et al. (2021) suggest several things related to information systems and technology in pandemic countermeasures. First, the availability of mobile applications can reduce risks and improve the way pandemics are handled. This application, or at least a site that can be easily accessed from mobile devices and easy to understand, will help monitor and convey information to the public. Second, big data is needed in analyzing and helping to predict environmental conditions. Third, the infrastructure of information systems also requires well-established resources so that the analysis and management of public information can be done quickly. The entire technology that is owned then needs to be integrated with business processes and human resources (He et al., 2021).

For this reason, building public information systems also needs certain consideration in terms of funding, infrastructure readiness, and human resource capabilities. The KIP Law has guided the provision of infrastructure in public information. At least, the availability of sites about public information in the agency is provided to make it easier for the public to find related information.

2. Process Management

The management of public information is focused on providing information to the public and an effort to achieve organizational goals. Thus, public information management requires alignment with organizational processes. Griffin (2004) explains that information management includes collection, control, and delivery. Information collection requires control in ensuring the information collected is as needed. Then, the information is integrated with the organization's system, and the information is used and managed by the purpose.

Furthermore, the information is conveyed to the audience to be utilized. Moreover, the processes that hinder public information management, such as hierarchies and bureaucracies in public institutions, can be overcome by the construction of internet-based information technology networks that allow every interested actor to respond to various issues in public information management. This requires procedures and adjustments to organizational characteristics (Sundgren, 2012).

a. Procedure

Public entities in Indonesia already have guidelines or references in implementing and managing public information. Referring to KIP law, PP no. 61 of 2010 and Information Commission Regulation (PERKI) No. 1 of 2010 can assist public bodies in making standard

procedures. In performing public information services, in principle, it is necessary to meet the elements of ease, speed, and accuracy.

Writing a procedure needs to adjust to the conditions and limitations that the organization has. Limits that are owned certainly need to be considered so that existing procedures can be modified but still meet the essence of managing public information without reducing the quality of service. The research results from Amali (2016) showed that the limitations of building facilities did not limit its public information service unit in Bitung. In addition, he also emphasized the need for consistency from the implementation of procedures so that transparency and accountability of public information are maintained in organizational dynamics. Furthermore, to draft regulations and procedures in participatory information management to shift the level of responsibility from institutional accountability from top-down to partnership approaches, where people increasingly take personal responsibility for limiting their exposure and vulnerability upon information.

b. Public Information Audit

One way to identify public information's risks and security aspects is to conduct an information audit. The concept of this audit is part of what the organization does in its operational activities. Although initially more critical to the financial aspect, now the audit also includes examination and details of non-financial elements, resources, and other activities in the organization (Milner, 2000). As it is well known, some organizations have International Standard Organization (ISO) certificates to ensure the quality of services are standardized and audited on an ongoing basis.

In the context of information, the audit focuses on a periodic review of information assets, identifying information-related problems, and measuring or defining the 'value' of existing information (Milner, 2000). However, Milner (2000) revealed that information auditing activities are potentially time consuming and expensive. To that end, organizational leaders will promote unusual ways to have organizations rate or measure 'value'. Perhaps ironically, it is a way of thinking that tends to be more easily accommodated and welcomed by public sector managers than in the commercial sector. It explicitly provides a base and guidance system for almost everything business-related. This is seen in the KIP Law were in determining whether information can be opened to the public or not is to test the consequences of information. In addition, through the Central Information Commission, the government also conducts monitoring and evaluation of public information every year to public entities. The results of evaluation and advice are then submitted to public entities to improve the quality of public information services.

To overcome the limited time and cost of conducting information audits, Milner (2000) suggests that before an audit is performed, organizations need to define the purpose of these activities through several things clearly. First, organizations need to understand how existing information processes support the organization’s goals. Next, identify the information required in re-engineering the organization's success. Finally, the organization needs to know the value of its information. The overall consideration is expected to result in a decision that applies at the macro and micro levels of the public service in question (Milner, 2000). For that, auditors need to build a specific strategy for public information. Jeppesen et al. (2017) suggest that it can be done by combining financial and performance aspects or even integrating financial, compliance, and performance parts.

Public information audits are conducted to show opportunities and reasons in supporting the provision of public information in improved information effectiveness, improvement of work quality and public information support systems. The organization is always required to question the quality and value of its information to internal and external customers. For this

reason, the audit questions the feasibility of technology and process and the quality of human resources that manage public information.

3. Human Resource Management

All public entities often have human resource issues, which become essential, especially in managing public information. Blakley et al. (2001) argue that managing information security and risk requires professional human resource with characteristics such as particular educational specialization, the permission of practice, control and keeping information secret, and understanding the ethics of information. These professionals are expected to identify information-related issues and manage them not to have the potential to harm the organization.

a. Training

Training is one of ways to overcome the disparity between reality conditions and the need for workers who have special skills, in this case, related to risk and security of public information. Puhakainen and Siponen (2010) stated that at least two things need to be met in organizing training. First, the training program, particularly in information security, should provide a theoretical explanation of how and why the training program is required. The material explains how people learn, and the learning principles that are expected to change user compliance with information security policies. As a second requirement, the underlying theory should guide how successful training is delivered in practice. This is important for practitioners who need practical guidance inadequate training. Furthermore, Puhakainen and Siponen (2010) also reminded that learning about risk and information security is ongoing. For this reason, training needs to be done periodically to increase capacity amid the development of information and technology that continues to grow.

In addition, Golding and Rubin's (2011) study shows that multicultural ability, culturally appropriate messaging, and the ability to collaborate with diverse communities are communication competencies required in risk management-related training for public information managers. Korpelainen and Kira (2010) mentioned that in addition to training, collaborating with colleagues and providing advice and guidance becomes very important in improving employee knowledge and information. Therefore, it is expected to assist educators in delivering materials and help them tailor training approaches to various organizations and target groups.

b. Leadership

As van Benthem and Martinez (2008) spell out, humans or agents have a spectrum of different attitudes toward information and have unlimited power over what they know. Thus, seeing that agents as members in an organization in information management has an important role. More specifically, leadership in information management plays an essential role in creating operational stability and implementing innovation processes and business strategies (Karahanna &Watson, 2006). In more detail, Karahanna and Watson (2006) explained that leadership in information management requires a combination of technical skills of information systems with an in-depth understanding of the various functions from operational to strategic of an organization. For this reason, the leader must be able to digest the current information, formulate, and then communicate the information to others in his efforts to achieve the organization's goals. The dynamics of information change in organizations are also continuously influenced by the internal environment, including structure, values, organizational culture, rules, and external environments such as culture, economic and political conditions. In addition, the ability in virtual leadership related to the ability to lead through technology with unlimited distance, space and time, is indispensable in this present (Christoffels, 2019).

Managing these dynamics requires leaders who can navigate to survive and face these challenges and changes. Therefore, individuals are inseparable from information, and the role of individuals or agents, especially in leadership, is vital in information management in an organization.

E. CONCLUSION

Technology that continues to develop needs to be utilized optimally to improve the quality of public information and reduce threats and risks from the information systems aspect. In addition, organizational processes also need to have holistic procedures and perspectives to make it easier to identify risks and formulate preventive measures (Figure 2).

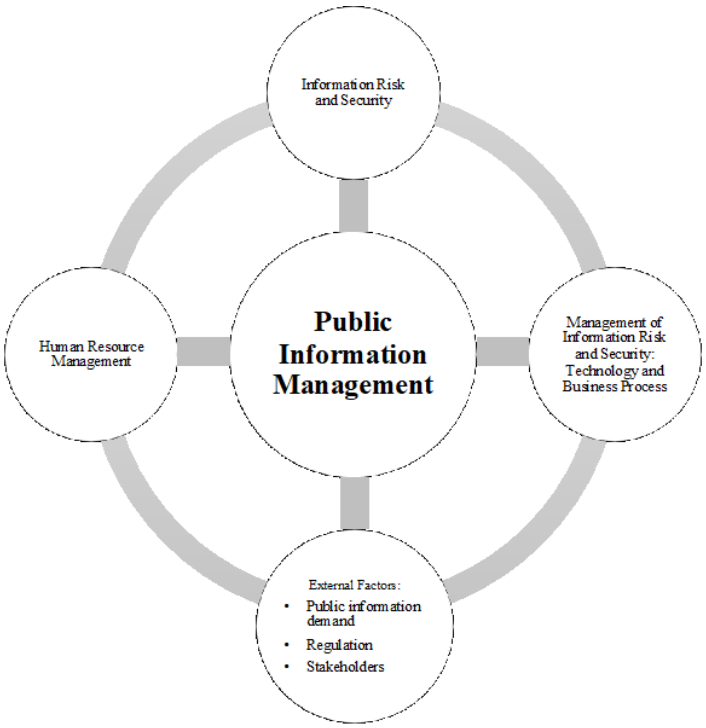

Figure 2. Conceptual Models in Risk Management and Public Information Security With a Holistic Approach

A holistic approach requires consideration in assessing the risks and security of information that comes from the data and information itself and the external environment such as regulation, building supporting infrastructure such as technology and information systems that also support the organization's business processes. Also importantly, human resources in public information risk management are needed in understanding, articulating, predicting, and delivering solutions. In particular, leaders of public entities need to understand the management of public information. They play a role in the control and decision-making related to managing public information and facilitators in translating organizational and public interests, conveying possible risks and offering solutions in managing public information amid the limitations and dynamics that exist. Integrating these various approaches is expected to illustrate more comprehensively for public organizations in organizing risk management and public information security.

A review of the literature related to the role of management in information security and risk shows that various management activities significantly impact the quality of public information management. Especially 1) the development and implementation of information security policies, 2) awareness, 3) compliance training, 4) effective enterprise information

architectures, 5) information systems infrastructure management, 6) business processes, and 7) human resource management. Through the constructed model, the study seeks to offer a more holistic approach to public information security and risk management and advises managers to play an active and effective role in managing public information. However, this study still has limitations, including keywords that focus on risk management and public information. Using other keywords such as government information management is expected to provide a richer picture of the study topic. This study also opens up further research opportunities in public information management, such as reviewing related elements in this research and conducting empirical studies quantitatively and qualitatively to explore the pattern of public information security risk management in public sector organizations

REFERENCES

Amali, S. (2016). Kesiapan PPID Dinas Komunikasi Informatika dalam pelayanan informasi publik (Kasus di Kota Bitung, Provinsi Sulawesi Utara). *Jurnal Penelitian Komunikasi Dan Opini Publik*, *20*(2), 123–140.

Avery, E. J., & Lariscy, R. W. (2011). Public information officers' perceived control in building local public health agendas and the impact of community size. *Health Communication*, *26*(8), 691–700. https://doi.org/10.1080/10410236.2011.563351

Bieri, F. (1994). Public information and the ethical responsibility of the industry. *Methods and Findings in Experimental and Clinical Pharmacology*, *16*(7), 491–496.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *Proceedings New Security Paradigms Workshop*, 97–104. https://doi.org/10.1145/508185.508187

Boserup, L. K., Christensen, J. P., & Pedersen, L. A. (2005). *An introduction to openness and access to information* (L. A. Pedersen (ed.). Danish Institute for Human Rights.

Bouhadana, I. (2016). The right of access to public information: an analysis of international conventions. *Revue Internationale Des Gouvernements Ouverts*, *2*, 1–10.

Campomizzi, A. J., Morrison, M. L., DeWoody, J. A., Farrell, S. L., & Wilkins, R. N. (2012). Win-stay, lose-switch and public information strategies for patch fidelity of songbirds with rare extra-pair paternity. *Scientific Reports*, *2*(294), 1–6. https://doi.org/DOI: 10.1038/srep00294

Christoffels, M. (2019). A framework for managing change leadership in a digital transformation environment. *Proceedings of the 15th European Conference on Management, Leadership and Governance, ECMLG 2019*, 428–437. https://doi.org/10.34190/MLG.19.011

Cochrane, T. A., Wicke, D., & O'Sullivan, A. (2011). Developing a public information and engagement portal of urban waterways with real-time monitoring and modelling. *Water Science and Technology*, *63*(2), 248–254. https://doi.org/10.2166/wst.2011.043

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth Edit). SAGE Publications, Inc.

Dunn, G., Henrich, N., Holmes, B., Harris, L., & Prystajecky, N. (2014). Microbial water quality communication: Public and practitioner insights from British Columbia, Canada. *Journal of Water and Health*, *12*(3), 584–595. https://doi.org/10.2166/wh.2014.126

Fakih, F., & Lawati, S. (2019). Keterjangkauan informasi dalam pelayanan publik. *Jurnal Ilmu Administrasi Dan Studi Kebijakan (JIASK)*, *2*(1), 1–7. https://doi.org/10.48093/jiask.v2i1.14

Galetta, D.-U. (2018). Access to administrative documents and to public sector information in Italy. In *The Right of Access to Public Information* (pp. 343–367). Springer.

Golding, L., & Rubin, D. (2011). Training for public information officers in communication to reduce health disparities: A needs assessment. *Health Promotion Practice*, *12*(3), 406–

413. https://doi.org/10.1177/1524839909344185
Griffin, R. W. (2004). *Manajemen*. Erlangga.
He, W., Zhang, Z. (Justin), & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International Journal of Information Management*, *57*(December 2020). https://doi.org/10.1016/j.ijinfomgt.2020.102287
Irianto, P. S., & Ispriyarso, B. (2016). Keterbukaan informasi publik di perbankan. *LAW REFORM*, *12*(2), 240–255.
Jeppesen, K. K., Carrington, T., Catasús, B., Johnsen, Å., Reichborn-Kjennerud, K., & Vakkuri, J. (2017). The strategic options of supreme audit institutions: The case of four Nordic countries. *Financial Accountability & Management*, *33*(2), 146–170.
Jonason, P. (2018). The Swedish legal framework on the right of access to official documents. In *The Right of Access to Public Information* (pp. 235–264). Springer.
Karahanna, E., & Watson, R. T. (2006). Information systems leadership. *IEEE Transactions on Engineering Management*, *53*(2), 171–176. https://doi.org/10.1109/TEM.2006.872247
Kaye, D. (1995). The importance of information. *Management Decision*, *33*(5), 5–12. https://doi.org/10.1108/EUM0000000003897
Kim, S.-B., & Kim, D. (2020). ICT implementation and its effect on public organizations: The case of digital customs and risk management in Korea. *Sustainability*, *12*(8), 3421.
Komisi Informasi Pusat. (2019). *Putusan Sengketa Informasi*. https://komisiinformasi.go.id/?p=3167
Korpelainen, E., & Kira, M. (2010). Employees' choices in learning how to use information and communication technology systems at work: Strategies and approaches. *International Journal of Training and Development*, *14*(1), 32–53. https://doi.org/10.1111/j.1468-2419.2009.00339.x
Lee, D. W. (2019). Can communication by the government improve trust and reduce risk perception? *International Review of Public Administration*, *24*(3), 190–204. https://doi.org/10.1080/12294659.2019.1645927
Lee, D. W., & Kwon, G. H. (2019). The effect of risk communication on the acceptance of policies for high-risk facilities in South Korea: With particular focus on the mediating effects of risk perception. *International Review of Administrative Sciences*, *85*(2), 337–355. https://doi.org/10.1177/0020852317702445
Lepesteur, M., Wegner, A., Moore, S. A., & McComb, A. (2008). Importance of public information and perception for managing recreational activities in the Peel-Harvey estuary, Western Australia. *Journal of Environmental Management*, *87*(3), 389–395. https://doi.org/10.1016/j.jenvman.2007.01.026
Linden, A. (1999). Overt intentions and covert agendas: Discourse on formulating communication policies and planning in third world countries. *Gazette (Leiden, Netherlands)*, *61*(2), 153–74. https://doi.org/https://doi.org/10.1177/0016549299061002004
Meijer, A., & Thaens, M. (2009). Public information strategies: Making government information available to citizens. *Information Polity*, *14*(1–2), 31–45. https://doi.org/10.3233/IP-2009-0167
Milner, E. (2000). *Managing information and knowledge in the public sector*. Routledge.
Morris, S., & Shin, H. S. (2002). Social value of public information. *American Economic Review*, *92*(5), 1521–1534.
Njenga, K., & Brown, I. (2012). Conceptualizing improvisation in information systems security. *European Journal of Information Systems*, *21*(6), 592–607. https://doi.org/10.1057/ejis.2012.3
Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, *3*(3), 398–427. https://doi.org/10.1287/orsc.3.3.398

Peltier, T. R. (2013). *Information security fundamentals*. CRC Press.
Perri, 6, Bellamy, C., & Raab, C. (2010). Information-sharing dilemmas in public services: using frameworks from risk management. *Policy & Politics*, *38*(3), 465–481.
Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, *34*(4), 757–778.
Rahmanto, N. (2021). Keterbukaan informasi publik data pertanahan. *Widya Bhumi*, *1*(1), 58–64.
Sexton, K. (2013). Evolution of public participation in the assessment and management of environmental health risks: A brief history of developments in the United States. *Journal of Public Health Research*, *2*(2), 18. https://doi.org/10.4081/jphr.2013.e18
Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management*, *14*(4), 225–239. https://doi.org/10.1007/s40171-013-0047-4
Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006
Spagnoletti, P., & Resca, A. (2008). The duality of Information Security Management: Fighting against predictable and unpredictable threats. *Journal of Information System Security*, *4*(3), 46–62. http://eprints.luiss.it/955/
Strauss, A. L., & Corbin, J. M. (1998). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (Second Edi). Sage Publications, Inc.
Sundgren, B. (2012). What is a public information system? *International Journal of Public Information Systems*, *1*(1).
Swiss, J. E. (2007). Information technology as a facilitator of results-based management. *Modern Public Information Technology Systems: Issues and Challenges*, 204–220.
Taylor, R. G. (2015). Potential problems with information security risk assessments. *Information Security Journal*, *24*(4–6), 177–184. https://doi.org/10.1080/19393555.2015.1092620
Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 Keterbukaan Informasi Publik, 5 (2008) (testimony of UU KIP).
van Benthem, J., & Martinez, M. (2008). The stories of logic and information. In P. Adriaans & J. van Benthem (Eds.), *Handbook of the Philosophy of Science* (Issue November, pp. 217–280). Elsevier Science Publishers. https://doi.org/10.1016/B978-0-444-51726-5.50012-1
Vaughn, R. G., & Messitte, P. J. (2018). Access to information under the Federal Freedom of Information Act in the United States. In *The Right of Access to Public Information* (pp. 191–234). Springer.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
White, J. D. (2015). Managing information in the public sector. In *Managing Information in the Public Sector*. https://doi.org/10.4324/9781315702650
Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. In M. E. Whitman & H. J. Mattord (Eds.), *Cengage Learning* (Fourth Edi).
Widodo, S. (2013). UU Keterbukaan Informasi Publik antara harapan dan kenyataan. *KANAL: Jurnal Ilmu Komunikasi*, *1*(2). https://doi.org/https://doi.org/10.21070/kanal.v1i2.333
Wieder, J., Protection, U. S. E., Washington, A., & States, U. (2018). Communication, education and public information for radiological emergencies: What is next? *Health Phys.*, *11*(4), 204–205. https://doi.org/10.1097/HP.0000000000000738.Communication