RISK DETECTION IN DIGITAL INFORMATION MANAGEMENT: A RECORDS MANAGEMENT PERSPECTIVE

Harry Bawono*

**The Center for Research and Archival System Development,*
The National Archives of the Republic of Indonesia
Email: harry.bawono@anri.go.id

DOI: 10.24252/kah.v8cf3

ABSTRAK: Peraturan Presiden tentang e-Government tahun 2018 menjadi titik awal percepatan implementasi e-Government di Indonesia. Momen ini mendorong instansi pemerintah berlomba-lomba mendigitalkan organisasinya untuk menerapkan regulasi tersebut. Informasi digital sebagai keluaran dari digitalisasi masif ini akan melimpah dan harus dikelola dengan baik yang tentunya rentan terhadap ancaman. Ancaman semacam itu dapat membahayakan keaslian catatan dan membuatnya tidak dapat dipercaya. Kerangka kerja deteksi risiko yang memadai yang sesuai dengan konteks lingkungan digital diperlukan untuk meminimalkan insiden ini. Kerangka kerja ini berisi perspektif manajemen arsip yang telah mengalami pergeseran paradigmatik. Kerangka kerja ini mengadopsi pandangan bahwa manajemen arsip merupakan bagian integral dari manajemen informasi digital. Studi ini menggunakan metode kualitatif dan menemukan bahwa dari perspektif manajemen arsip, kerangka kerja deteksi risiko dalam manajemen informasi digital menyoroti aspek konteks (eksternal dan internal), sistem, dan proses. Namun, kelancaran implementasinya di lingkungan digital, khususnya di Indonesia, ditentukan oleh sejauh mana reformasi paradigmatik dalam pengelolaan arsip telah berlangsung.

Kata kunci: e-Government; Lembaga pemerintahan; Lingkungan digital; Infomasi digital; Manajemen arsip; Resiko

ABSTRACT: *The Presidential Regulation on e-Government in 2018 became the starting point for accelerating e-Government implementation in Indonesia. This moment prompted government agencies to compete in digitizing their organizations to apply the regulation. Digital information as the output of this massive digitalization will be abundant and must be managed properly which is certainly vulnerable to threats. Such threats can compromise the authenticity of records and make them untrustworthy. An adequate risk detection framework that fits the context of the digital environment is needed to minimize these incidents. This framework contains a records management perspective that has undergone a paradigmatic shift. This framework adopts the view that records management is an integral part of digital information management. The study used a qualitative method and found that from the perspective of records management, the risk detection framework in digital information management sheds light on aspects of context (external and internal), systems, and processes. However, its smooth implementation in the digital environment, especially in Indonesia, is determined by the extent to which paradigmatic reforms in records management have taken place.*

Keywords: *e-Government; Government agencies; Digital environment; Digital information; Records management; Risk*

1. INTRODUCTION

The digitalization of government business processes has been re-echoed since the issuance of Presidential Regulation Number 95 of 2018 concerning the Electronic Government (e-Government). Later, through e-Government, every government organization will use ICT

(digital information system) to operate their business. In the e-Government, the non-digital system that has been used will change to a digital system. Thus, digital information or records becomes valuable resources that should be managed by those organizations. One field which is concern about this issue is records management.

The problem is that the management of digital information requires a complex digital records management system and cannot be simplified by simply installing an electronic office information system (e-office) (Bawono 2017). There are significant differences between the digital and non-digital information landscape. Information forms in the digital information landscape are more diverse and complex. Therefore, it needs a different schema than before.

An issue that is often overlooked, especially by the government agencies, and is crucial in a digital environment is a risk. The digital environment is much more vulnerable than the non-digital environment (PARBICA 2004). The digital environment is barely controlled, making all forms of digital information face various threats that can damage their authenticity. When the authenticity of information is damaged, it can no longer be trusted.

Nevertheless, the general risk management concept in government agencies has been regulated by the Financial and Development Supervisory Agency/*Badan Pengawas Kekuangan dan Pembangunan* (BPKP) as appear in its regulation concerning risk-based internal supervision (BPKP 2018). Likewise, the concept of risk management in records management has been briefly described by the National Archives of the Republic of Indonesia/*Arsip Nasional Republik Indonesia* (ANRI) on its regulation Number 24 of 2011 concerning Guidelines for Organizing Archives in Higher Education Environment (ANRI 2011). However, the risk detection scheme in this regulation needs improvement because it still too general and simple, so it needs to be developed into a more specific and comprehensive regulation on risk assessment or detection that is adaptable for managing digital information.

In a digital environment, the value of information equal to oil that could turn on the machine. Thereby, it is not surprising that information is currently perceived as an organizational asset, as reflected in the definition of the records listed in ISO 15480-1: 2016 (ISO 2016). In this context, damage and loss of information mean the loss of organizational assets. Concerning those issues, risk detection is important to do to minimize damage and loss. Through this risk detection, risk management can be carried out. Then, how is the risk detection scheme from the records management perspective that could be implemented for managing digital information in the context of e-Government in Indonesia?

The objective of this research was to describe the perspective of records management to detect risks in managing digital information in the context of e-Government. That way, this study could use by the government agencies as a reference in developing risk detection policies in managing digital information in their respective environments.

2. METHOD

This research was conducted using qualitative methods through literature studies, interviews, and Focus Group Discussion (FGD). The data collection was conducted from January to November 2019. The informant was involved in this research including government officials and experts from a non-government official. For the informant from the government official group, the selection is based on the following criteria, such as mastering the concept of risk management within government agencies. Meanwhile, for the non-government group, an informant was selected based on the following criteria, such as experts or practitioners who master digital records management, information technology risk management. Informants involved in this research can be seen in the table 1.

Table 1. Informant

No	Informant	Interview
1.	Informant A, ExxonMobil Cepu, Unit of	8-12 April 2019

No	Informant	Interview
	Document Controller	
2.	Informant N, BPKP, Jakarta	23-24 Mei 2019
3.	Informant F, Expert of Information Security	5 November 2019

The researcher processed the finding data and information with selection, reduction, categorization, and conceptualization. The researcher selects the finding data by grouping it which was relevant and which was not relevant to this research. The irrelevant data were reduced and not used in this research. Meanwhile, the relevant data were analyzed then conceptualized by synthesizing the finding data with a conceptual framework constructed by the researcher.

3. RESULTS AND DISCUSSION

Digital Information Landscape and its Translation to e-Government

Referring to the ISO 15489-1: 2016, records are defined as information created, received, and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business (ISO 2016). Specifically, electronic (digital) records can be conceptualized as records that are born digitally, for example in computer-based information systems (Duranti, 2001) or records that are born in other digitized formats (Borglund, 2007).

These records are managed in a records management system. In general, the records management system is divided into two types, non-digital and digital. In a non-digital records management system, records are not managed using digital information systems (software). Meanwhile, in the digital/electronic records management system, a computer program, or a set of computer programs used to manage records stored in related databases (Kingdon, 2012). This management system starts with access control, auditing, and also the destruction process (Kingdon, 2012). Due to its vulnerable nature, digital records management requires a sustainability scheme. This continuity scheme is usually integrated into information governance.

The development of digital records in parallel with the development of ICT, the more complex the development of ICT, the more complex the digital records are. In simple terms, the form of digital records can be divided into 4 (four) categories (Katuu 2016):

a) Document created using office applications (Word, Powerpoint, Excel etc);

b) Records generated by business information systems;

c) Records in online and web-based environments;

d) Electronic messages from communications system.

For more details, see table 2.

Table 2 Form of Digital Records

(A)	(B)
Document created using office applications (Word, Powerpoint, Excel etc): - word-processed document; - spreadsheets; - presentations; - desktop-published document	**Records generated by business information systems:** - database - geospatial data systems - human resources systems - financial systems - workflow systems - client management systems - customer relationship management systems - systems developed in-house

	- content management systems
(C) **Records in online and web-based environments:** - intranets - extranets - public websites - records of online transactions - (social media)	(D) **Electronic messages from communications system:** - email - SMS (short messaging services) - MMS (multimedia messaging services) - EDI (electronic data interchange) - electronic document exchange (electronic fax) - instant messaging - EMS (enhanced messaging services) - multimedia communications (eg video conferencing and teleconferencing)

Source: (Katuu 2016)

The four forms of digital records were born and then managed in a digital information system. In this context, Borglund (2006) wrotes, in a digital environment, records production will take place through various information systems, so the quality of digital records will depend on the quality of the information system. This argument implies that the management of digital records is also the management of information systems that produce and also manage these digital records.

With the evolving state of digital records, the evolution of digital records management could be tracked into, at least, in three phases (Katuu 2012):

1. Electronic Document Management Systems (EDMS), Electronic Records Management Systems (ERMS);
2. Integrated Document and Records Management Systems (IDRMS), Electronic Document and Records Management Systems (EDRMS);
3. Enterprise Content Management Systems: Document Management, Records Management, Workflow, Bussines Process Management (BPM), Knowledge Management (KM), Portal.

In the Indonesian context, the development of such a digital environment is then translated into the e-Government program. In this program, one of the domains of concern is the management of digital records. The management of digital records planed to be developed is integrating Official Electronic Documents System (integration of e-office) (KemenPANRB 2019). When it concept analyzed to table 2, the digital records management currently developed is still focused on the category (A).

When that problem is viewed from the perspective of the development of the digital records management phase, based on the author's involvement in various meetings about e-Government, the current condition of e-Government is still in phase (2). Although the foundation for phase (1) is not yet well-established. The fundamental problem that must be addressed is the domination of the category (A) (see table 2) records management paradigm implant by the government agencies. Besides, paradigmatically, they still identify digital records management with non-digital records management. Accordingly, it is not surprising when government agencies still find it difficult to imagine a digital records management illustrated in phase (3).

Referred to Bearman (1993), a new environment needs a new paradigm. The implement of the old paradigm to a new environment would hamper the digital records management itself (Duranti 2001). The first step that should be taken to overcome this problem is to shift a non-digital (paper-oriented) to the digital paradigm(Cook 2007).

The agencies would find various challenges in the digital environment that have never been found before. Those various challenges only could identify when the agencies apply the new paradigm. Furthermore, when the agencies are not comprehensively implemented the new

paradigm, it would make the digital records management practice difficult to improve from one phase to another phase. Moreover, the agencies would hard to develop a system that captures all categories of digital records, as reflected in table 2. Then, the unchanging paradigm will make various kinds of digital records in the agencies unseen from the radar. When those records are unrecognized, the potential for government agencies to lose their digital information assets is even greater.

Context and Why Risk Detection in Digital Information Management is Critical

The concept of risk analysis began to be widely discussed and became part of the institutions of modern society since the 1970s (Berner 2003, 4). Many actors are involved in the use of this risk analysis as part of their efforts to define uncertainty and risk in the lives of modern societies in which technology is inherent (Berner 2003, 4).

Risks are related to what is constructed as a risk, who is constructs it, and how the risks are systematized in such a way as to be managed or ignored altogether (Berner 2003). Due to risk is a matter of social construction, it always relates to negotiations between various views and power relations. So it is not surprising that in the organizational context, leaders and staff have a different angle to define what is treated as a risk or no risk at all.

In the field of information management, including records management, the concept of risk is congruent with the development of ICT. This makes the volume and diversity of information grow rapidly. Such conditions require a complex mechanism to control and manage that information (IronMountain 2015). This mechanism is substantial due to the information is new resources that are very useful for human life in the information era (Woodal 2014, 5). If the mechanism operates improperly, our efforts will only be in vain because only managing valueless information (Woodal 2014, 5).

With the condition of the rapid development of ICT, it is encouraging organizations to adapt by making changes from managing non-digital to digital records. In making these changes, of course, a framework is needed to deal with risks that are fundamentally different from managing non-digital records (Egbuji 1999). In his research, Egbuji (1999) illustrates these three risks:

1) Passive intrusion: this can be done through wiretapping and impersonating a valid user. Authorized users and operators are often unaware of this;
2) Active intrusion: this includes actions such as hacking, deleting, or falsifying records, entering redundant information, or malicious viruses into the network to disrupt the network.
3) Sabotage: the threat of damage due to deliberate or unintentional actions to disrupt and damage the system will cause fatal damage. The research found that only 1 in 4 organizations succeed in survives after experiencing severe damage due to this sabotage.

Indonesia is one of the countries that are passionate about digitalization jargon as a package in industry 4.0. As a result, every organization, both private and government, is competing to digitalizing their business. Concerning the risk management issue in the Indonesian case, it is important to cite the survey conducted by the Center for Risk Management Studies (CRMS) in 2019. The survey found, it is known that 76% of both private and government organizations answered that they had implemented integrated risk management, while 24% had not yet implemented it (CRMSIndonesia 2019). Furthermore, the extent to which the application of risk management takes place in Indonesia. The survey identified three conditions (CRMSIndonesia 2019):

1) Optimal, integrated principles and processes (33%);
2) Standardized, written principles and basic training (35%);
3) Informal and basic training (32%).

The survey also found the three most common obstacles face the respondents, namely the absence of a road map in the organizational strategy (33%), lack of adequate resources (human resources, budget, technology) (31%), and lack of sufficient information and training (21%), and others (15%) (CRMSIndonesia 2019).

CRMS's survey findings are very important for intake in making future improvements. Improvements can be made by overcoming these barriers so that the percentage of organizations implementing risk management continues to increase, from informal and basic training to standardized, and from standardized to optimal.

Specifically, for the government agencies cases, the Financial and Development Supervisory Agency/*Badan Pengawasan Kekuangan dan Pembangunan* (BPKP) has issued a risk management instrument for government agencies in the form of a Government Regulation Number 60 of 2008 concerning Government Internal Control Systems/*Sistem Pengendalian Internal Pemerintah* (SPIP). Each government agency implements this regulation through its inspectorate unit. In ensuring the implementation of risk management in each government agency, BPKP evaluates it by giving certain predicates which are divided into 6 levels, as mention by Informant N (Interview, Informant N, Jakarta, 23 May 2019):

> *"nantinya ketika penilaian sudah dilakukan, akan diketahui masuk dalam kategori apa…apa tidak ada sama sekali..ada tapi tidak sistematis atau ad-hoc aja..kemudian, beru awal pengembangan tapi tidak terdokumentasi secara layak..atau sudah berjalan atau terdefinisi, ini dibagian evaluasi belum terdokumentasi..lalu sudah terkelola dan terukur…dokumentasi di proses dan evaluasi sudah berlangsung..selanjutnya optimal, kalo ini berkelanjutan, monitor dan evaluasi sudah rutin…"*
>
> (translation: Later, when the assessment has been carried out, it will be known what category it belongs to ... is it not manage at all ... is there but not systematic or ad-hoc ... then, the beginning of development is not properly documented ... or has been running or defined, this is in the evaluation section it has not been documented ... then it has been managed and measured ... the documentation in the process and evaluation has been carried out ... then, if it is optimal, it is mean the process is regularly running, monitoring and evaluation are routine ...)

Based on this cited, formally, the 6 level categories are:

1) Not available (there is no SPIP policy and procedure);
2) Stubs (ad-hoc and unorganized);
3) Developing (running but not yet documented and evaluated);
4) Defined (running documented but the evaluation not documented);
5) Managed and Measurable (effective, documented, evaluation formally documented);
6) Optimum (continuous, integrated, routine monitoring/evaluation).

The problem that is often encountered by the agencies related to risk management is its mechanism often only exists in a document, but not in practices. Government agencies have indeed documented risks and all forms of mitigation, but this has not been applied systematically. As said by Informan N (Interview, Informant N, Jakarta, 23 May 2019):

> "*dari hasil asesmen ini ... biasanya instansi pemerintah, manajemen risiko sudah memiliki dokumen, tapi ya ... belum sinkron dengan tataran praktis dan tidak sistematis*"
>
> (translation: From the results of this assessment ... usually in government agencies, the are a document of risk management, but it was not synchronized with the practical level and not systematic at all)

There are many factors, one of which is the absence of more specific guidelines for certain domains, for example, the records management field. Formal guidelines for risk assessment for

digital information management (digital records management) as integral to the macro of risk management have not been prepared to date. This guide is very important because a macro risk management scheme, risk management of this kind is an integral subsection therein. The success of macro risk management is also closely related to this kind of micro-level risk management. This perspective was expressed by Informant N (Interview, Informant N, Jakarta, 23 May 2019):

> "*Jadi ini bagus ini..kalo ada inisiatif menyusun manajemen risiko pada bidang apa itu yang spesifik atau lebih mikro..karena ini akan membantu dalam skema manajemen risiko yang makro..nantinya ini akan saling mengisi dan kesuksean implementasi mnajemen risiko di bidang mikro ini berkontribusi pada manajemen risiko yang makro, jadi..kita tunggu juga ini,,,"* (translation: So this is great ... if there is an initiative to compile risk management in what is a specific or more micro field ... because this will help in a macro risk management scheme ... later this will complement each other and the success of risk management implementation in the micro sector will contribute to macro risk management, so ... we'll also wait for this,,,)

With such an illustration, risk management in digital information management (read: digital records) is basically for the survival and sustainability of the digital records itself (TheNationalArchives 2017). By understanding risk management, the organization's confidence in achieving organizational goals will be much more mature (TheNationalArchives 2017). Because without this expertise every organization will fail to protect its digital records (TheNationalArchives 2017). When it fails to protect digital records which are organizational assets, the organization fails to carry out its organizational functions.

In managing risk, each organization identifies and then assesses the identification results in a certain measure. The assessment by entering certain measures is done as a way to calculate the risk as real as possible. Thus, this vulnerability or uncertainty is relatively certain and ready to be overcome when it occurs.

The transform from managing non-digital to digital records is a form of digitalization. In the digital world, digital risks arise. Here, in the risk management perspective perceived the information as a digital asset. Digital assets are included in anything that is processed or exchanged. These digital assets are the results of the organization's business processes that are the object of risk analysis. The risk assessment will focus on weaknesses, for example, the condition of human resources who have not received training. This description was statement by Informan F (Interview, Informant F, Jakarta, 5 November 2019):

> *"Risiko digital mulai muncul ketika informasi yang non-digital menjadi digital, nah dari sini perspektif manajuemen risiko adalah informasi sebagai aset digital…Aset digital termasuk didalam apapun yang diolah, dipertukarkan…. Aset digital ini yang hasil dari proses bisnis organisasi yang menjadi focus asesmen risiko… Asesmen risiko nantinya focus pada kelemahan, misalnya kondisi sumber daya manusia yang belum mendapat pelatihan"*
>
> *(*translation: Digital risks begin to emerge when non-digital information becomes digital, so from here, the risk management perspective is information as a digital asset… Digital assets are included in anything that is processed or exchanged…. These digital assets are the results of the organization's business processes which are the focus of risk assessment ... The risk assessment will focus on weaknesses, for example, the condition of human resources who have not trained)

Mapping the risks is important at the beginning before the work process starts by identifying the business processes that have been running so far. Find the most detailed possible risks, make sure nothing is overlooked. Then, rank the risks from critical to minor, for the lightness risks can be put aside. Risk is always related to the internal and external conditions of the organization. Informant F described this process as mentioned on this quote (Interview, Informant F, Jakarta, 5 November 2019):

> *"Peta risiko sebaiknya disusun diawal sebelum proses kerja berjalan dengan mengidentifikasi dari proses bisnis yang berjalan selama ini… Temukan risiko sedetail mungkin, pastikan tidak*

ada yang terlewat…Urutkan risiko dari mulai kritis hingga ringan, untuk ringan bisa dikesampingkan… Risiko selalu berkaitan dengan kondisi internal dan eksternal organisasi"

(Translation: The risk map should be prepared at the beginning before the work process starts by identifying the business processes that have been running so far ... Find the most detailed possible risks, make sure nothing is overlooked ... Sort the risks from critical to mild, for the mild can be put aside ... Risk is always related to internal and external conditions of organizations)

The risk management perspective in the digital field is currently expanding, previously it focused more on the interests of information security, now it is heavier on cybersecurity, as mention by Informant F (Interview, Informant F, Jakarta, 5 November 2019):

"Perspektif manajemen risiko dunia digital saat ini meluas ya…sebelumnya itu kan lebih ke kepentingan keamanan informasi, saat ini lebih berat pada keamanan siber…"
(Translation: The perspective of risk management in the digital field is currently expanding, right ... before that it was more in the interests of information security, now it is heavier on cybersecurity ...)

Information security focuses on the substance of the information. Meanwhile, cybersecurity besides information also includes infrastructure. Because of these two things, information and infrastructure are closely related in determining cybersecurity as a whole. This context also needs to be seen in looking at the case of the National Archives (ANRI) which also focuses on digital preservation. Thus, Informant F explains more as in the following quote (Interview, Informant F, Jakarta, 5 November 2019):

"…jadi keamanan informasi fokus kepada substansi informasinya…nah, keamanan siber selain informasi juga meliputi infrastruktur….. Karena dua hal ini, informasi dan insfrastruktur saling berkaitan erat dalam menentukan keamanan siber secara keselurahan….Konteks ini juga perlu dilihat misalnya, dalam melihat kasus Arsip Nasional nih yang juga fokus pada preservasi digital"
(Translation: ... so information security focuses on the substance of the information ... well, cyber security besides information also includes infrastructure ... Because of these two things, information and infrastructure are closely related in determining overall cybersecurity .... This context also needs to be seen for example, in looking at this National Archives case which also focuses on digital preservation)

Information risk management revolves around three main concepts, threats, weaknesses, and controls. Risks can appear either positive or negative. Negative impacts on losses, positive impacts on profits. As an illustration, maintaining regularly the organization's equipment will make those tools protected from the damage. When the damage is reduced, the organization's expenses will also be depressed. The consequences, the structure of the organization's finances would be healthier.

It is not easy to control and understand the threat without a frame. In this position, the risk management framework is very important, because it institutionalized the planning, reporting, and evaluating process into an integral system. In this system, after risk analysis, it is regulated who will receive the report, the appropriate treatment to be taken to respond to the results of the risk analysis, echo the treatment taken towards the identified risks. Risk management often cannot be measured quantitatively. This issue explained sharply by Informant F as quoted below (Interview, Informant F, Jakarta, 5 November 2019):

"Begini…melakukan kontrol belum tentu mudah dan murah, intinya pahami terlebih dahulu ancamannya..Pada posisi ini kerangka kerja manejemen risiko sangat penting, karena dalam kerangka ini manajemen risiko terinstitusionalisasi dari proses perencanaan, pelaporan dan tindak lanjut dari laporan tersebut…Dalam sistem ini, paska analisis risiko, diatur siapa pihak yang akan menerima laporan, sikap yang selayaknya diambil untuk menyikapi hasil analisa risiko, tindak lanjut dari sikap yang diambil terhadap risiko yang telah teridentifikasi

tersebut…Persoalanya seringkali pengelolaan risiko ini tidak bisa diukur secara kuantitatif, bagaimana misalnya mengukur selama sebulan ini keamanan risiko membaik atau memburuk?

(Translation: Well ... doing control is not necessarily easy and cheap, the point is to understand the threat first ... In this position the risk management framework is very important, because in this framework risk management is institutionalized from the planning, reporting and follow-up process of the report ... In this system.. post risk analysis, it is regulated who will receive the report, the appropriate attitude to be taken to respond to the results of the risk analysis, follow-up on the attitude taken towards the identified risks ... The problem is often this risk management cannot be measured quantitatively, how for example measuring during this month the risk of security improved or worsened?)

There are two general approaches to calculating risk, processes and assets. The process approach would be observing the entire organizational process, but it rather difficult to fit into the asset level. At the asset level, it will be difficult to identify the process, for example, how many work processes being connected to one server? Usually, one server is used for several work processes. Informan F giving his opinion as mention below (Interview, Informant F, Jakarta, 5 November 2019):

"Dalam mengkalkulasi risiko ada dua pendekatan umum, proses dan asset…Proses dengan melihat keseluruhan proses organisasi, tapi agak sulit menurunkannya hingga tingkat aset… Aset akan kesulitan mengidentifikasi proses, misalnya sebuah server ini terhubung dalam berapa proses? satu server biasanya digunakan untuk beberapa proses kerja"
(Translation: there are two general approaches for calculating risk, processes and assets…A process by looking at the entire organizational process, but a little difficult to bring it down to the asset level…..The asset will have difficulty identifying the process, for example, a server is connected in how many processes? one server is usually used for several work processes)

However, there is a formula for determining the value of risk, the value of risk is equal to impact multiplied by possibility (risk value = impact x possibility). This risk value grades from crucial to insignificant. There are various risks, for example, for digital records, it can not only focus on digital documents, but all factors related to digital documents. This explanation gives by Informant F as quote below (Interview, Informant F, Jakarta, 5 November 2019):

"…ada formula yang biasa digunakan untuk menentukan nilai risiko, nilai risiko sama dengan dampak dikali kemungkinan…. Nilai risiko mulai dari krusial hingga tidak penting… Risiko itu dimensinya banyak, misalnya untuk dokumen digital, tidak bisa cum fokus pada dokumen digitalnya doang, tapi semua faktor yang berkaitan dengan dokumen digital itu"
(Translation: … There is a formula that is usually used to determine the value of risk, the risk value is equal to the impact multiplied by the probability…. The value of risk starts from crucial to insignificant… There are many dimensions of risk, for example for digital documents, you cannot focus on the digital document alone, but all the factors related to the digital document)

Organizations need to define the risks in detail. When you just make a summary it is worried that you will miss a lot of things. All risks must be considered. In the risk management point of view, impossible does not exist, every risk has a probability to happen. The case of an airplane crashing into the WTC building, United States, is a clear example of this case. The case proves that even though the occurrence is very rare, the damaging effect probably could be fatal. In this context, mitigation strategies should be considered. If it is rare and the effect is small, it can be left alone as long as it is controlled. The Informan F described these informations as cited below (Interview, Informant F, Jakarta, 5 November 2019)

"Menghitung risiko harus detail ya… jangan cuma ringkasan. Kalo hanya ringkasan banyak hal yang akan terlewat deh… Selain itu, semua risiko harus dipikirkan, karena ada yang dianggap tidak mungkin terjadi tapi ternyata kejadian, lihat itu kasus pesawat ditabrakan ke gedung WTC, Amerika Serikat….. Ini bisa jadi pelajaran, jeli ngeliat probabilitas risiko yang akan terjadi….Jika secara kejadian sangat jarang tapi efeknya besar, strategi mitigasi patut

dipikirkan, jika jarang dan efeknya kecil, bisa dibiarkan selama terkendali..agar tidak kaget kalo beneran kejadian"
(Translation: Calculating the risk has to be detailed ... don't just summarize ... If it's just a summary, you will miseed many things ... In addition, all risks must be considered, because something was deemed impossible then it turned out to be a real incident, look at the case of the plane crashing into the WTC building, United States… .. This can be a lesson, be aware of the probability of the risk that will occur…. If the incident is very rare but the effect is large, mitigation strategies should be considered, if it is rare and the effect is small, it can be left under control .. so as not to be surprised if it really is incident)

Informant F then explain the important of controls mechanism should be. In his point of view, controls mechanism needs to be sorted into three categories which are administrative, logical, and physical, as following quote (Interview, Informant F, Jakarta, 5 November 2019):

"..Kontrol ini penting..biasanya kontrol itu dibagi berdasarkan administrative, logis sama fisik.."
(Translation: ... control is important ... usually the control is divided based on administrative, logical and physical ...)

Administrative control, for example, if they want to access WiFi, they must submit a copy of their identity. Logical control, for example, to access wifi must use a username and password. Physical control, for example, the wifi network is secured by physically locking the server, the security of electricity intake or another action. The objective of the control mechanism is to predict, detect, and correct. The control mechanism could prevent something to happen in a term that the potential risk will define before it becomes the actual risk. The control mechanism could detect the risk using an assessment instrument, in consequence, the assessor could detailing the risk. Based on the successful detection, the corrective action will be easier to do by the organization when an incident occurs.

Another significant issue relates to the risk management field is about efficiency. How efficiently can you provide when it mechanism consistency implement to an entire organization, for example, when one company does not install antivirus compared to others who are installing it. The degree of efficiency strongly relates to the strategy would take by the organization. The case of Boeing Corporation could be a good example of illustrating this problem. The Boeing Corporation still use an old chipset computer system for their aircraft. They do not want to replace it with the current technology, because it is more complicated and needs a huge budget. On the other side, the old engine is no longer produced by the factory. Boeing decides a strategy after defining the risk. They choose to buy the entire stock of the old chipset directly from the factory then preserved it in a special room. The preserved stocks would use when the broken chipset needs to replace. The Boeing case was interestingly conveyed by Informant F (Interview, Informant F, Jakarta, 5 November 2019):

" Isu lain yang pasti muncul adalah tentang efisiensi, seberapa besar efisiensi misalnya, ketika satu perusahaan tidak menginstal anti virus dibandingkan dengan menginstal. Ini semua tentang strategi, contoh kasus Boeing, sistem komputer pesawat boeing masih menggunakan mesin lama, untuk mengganti system baru, lebih rumit dan butuh biaya besar, sementara mesin lama sudah tidak diproduksi, hal yang dilakukan boeing adalah memborong chipset mesin lama tersebut langsung dari pabriknya dan menyimpan di ruang khusus, ketika ada yang perlu diganti maka persediaan tersebut yang dimanfaatkan. Kasus Boeing menandakan bahwa tidak harus selalu mengikuti teknologi, yang penting adalah cara dan strategi untuk mengatasi keusangan teknologi tersebut"

(Translation: "Another issue that definitely arises is about efficiency, how big is the efficiency, for example, when a company does not install anti-virus compared to installing. This is all about strategy, for example in the case of Boeing, the Boeing airplane computer system still uses the old engine, to replace the new system, it is more complicated and needs a huge budget, while the old engine is no longer produced, what Boeing did was buy the old engine chipset directly from the factory. and store in a special room, when something needs to be

replaced then that stored chipset is used. The Boeing case indicates that we do not have to always follow technology, what is important is the way and strategy to overcome the obsolescence of technology "

From the Boeing case, it can be learned that what is important is the method and strategy tp tackle technological obsolescence. Another case that is important to describe is ExxonMobil. ExxonMobil chooses to continue managing non-digital records as part of its business continuity strategy hand in hand with the digital system. Therefore when the digital records management system collapse, the organization could still access and use their information or records. This issue described by Informant A as following cited (Interview, Informant A, Cepu, 8-12 April 2019):

"..Kami ini meskipun sudah mengelola rekod digital..tapi pengelolaan rekod non-elektronik tetap kami jaga..jadi ini kayak bagian business continuity plan, misalnya, sistem digital mengalami gangguan maka informasi tetap dapat diakses..."

(Translation: "Even though we have managed digital records ... we are still managing non-electronic records ... so this is like a part of the business continuity plan, for example, when the digital system is disrupting so information can still be accessed ..."

The biggest problem in risk management is that the organization does not recognize the risks that (will) exist surrounding their organization so that they missed many things to calculate. To tackle this problem, there is a matrix that is commonly used to detect the risk. This matrix would guide the organization to identify common information security risks. This matrix must be established by the leadership, openly to be updated, but not to change frequently. The focus depends on the needs, it shows the risks issues have its boundaries and need to be specified, for example, digital preservation.

Risk Detection Framework from a Records Management Perspective

The main purpose of (digital) records management is the sustainability of record authenticity (Anderson 2015). Sustainability of record authenticity is the continuity of a record quality since it was created and immune from corruption and disruption (Duranti and Blanchette 2004). This authenticity is not something singular condition, but a consequence of the various relationships surrounding the records (Rogers 2015). In this way, to maintain the sustainability of records authenticity, it is necessary to be intensive in mapping all kinds of relationships that affect the quality of the records. This can be facilitated through the detection of risks in various aspects that can affect the quality of the records. In this position, a risk detection framework in digital information management is very important.

From the perspective of records management, the risk detection framework is formulated in ISO/TR 18128 concerning risk assessment for records processes and systems. Referring to this framework, risk assessment in the records management process and system includes (ISO 2014):

a) Risk identification. Risk identification is the activity of searching for or describing certain aspects to find risks.
b) Risk analysis. Risk analysis is an activity to analyze findings in the risk identification section. When the analysis is carried out, risks are grouped as such and assigned a value based on their frequency of occurrence and impact.
c) Risk evaluation. Risk evaluation is the act of systematizing the identification that has been carried out against risks by grouping them according to the target aspects of risk identification, the likelihood and impact of these risks.

Risk identification. Risk identification is carried out by analyzing risk sources. Sources of risk are classified into three groups: Context (external and internal), System and Process. As reflected in Figure 1.

Figure 1. Risk sources
(Source: adapted from (ISO 2014)

External context is a condition that occurs outside the organization but will affect organizational conditions. External includes the following areas of uncertainty, sociopolitical change, macroeconomic and technological environment, physical environment and infrastructure, security. Social and political changes, for example, the existence of new regulations issued by the government that can affect the management of information/records. Macroeconomics and the technological environment, for example, economic crises that affect organizational priorities, new technologies circulating in society. Physical environment and infrastructure, for example, natural disasters, electricity disturbances. Security, for example, hacking and destroying the system by outside parties who access illegally, espionage, cessation of services from third parties, while the system built by it is still used by the organization. A summary of the sources of external risk can be seen in figure 2 below.

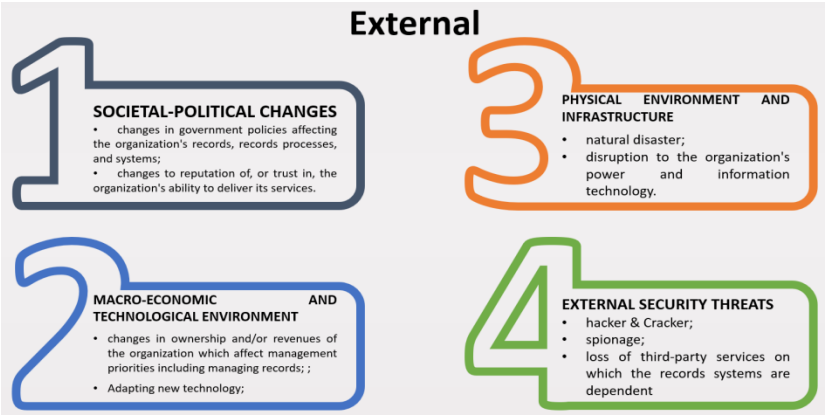

Figure 2. Areas of uncertainty: External
(Source: adapted from (ISO 2014)

Internal context is a condition that occurs within the organization which certainly affects the organization. Internal includes the following areas of uncertainty, organizational change, technology change, human resources, and funding. For example, organizational changes, there is the dissolution of a unit or organization or a merger of units or organizations, personnel moving or retiring. Technological changes, for example, changes in technology have an impact on system interoperability and compatibility, new technology means new regulations. Human resources, for example, the number of personnel, level of awareness, or knowledge of information/records

management, personnel digital competency. Funding, for example, the adequacy of funds for the records management program, the adequacy of funds for the improvement of facilities and infrastructure. A summary of the sources of internal risk can be seen in Figure 3 below.

Figure 3. Areas of uncertainty: Internal
(Source: adapted from (ISO 2014)

The records system. This system covers the following areas of uncertainty: design, maintenance, sustainability, interoperability, and security. Design, for example, the scope of the archive definition used, the retention system, the level of dependence on the vendor, access to vendor documents when building this system. Maintenance, for example, guarantees the continuity of the renewal system, backup system. Sustainability, for example, system specifications, system capability to maintain the usability of records, migration systems. Interoperability, for example, identification of the records management system interoperability with other business systems, the effectiveness of updated system interoperability levels, metadata systems. Security, for example, security regulations on records, processes, and systems, access to files, processes, and systems, regulation of third parties employed against the system. A summary of the sources of system risk can be seen in Figure 4 below.

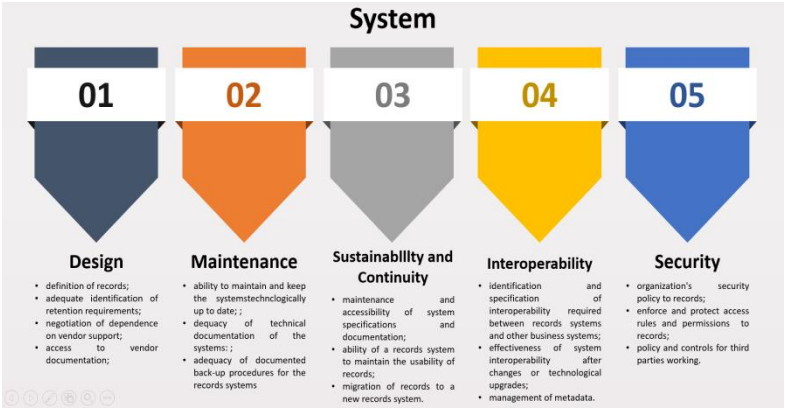

Figure 1 Areas of uncertainty: System
(Source: adopted from (ISO 2014)

In the process section, it focuses on the creation of elements and the process of controlling records and the archive management system. The process includes the following areas of

uncertainty: system design, creation, and implementation, metadata, use and system records, maintenance of usability, process depreciation. Design, for example, analysis of activities to map records created, metadata, process descriptions, the process uses, naming classifications. System creation and implementation, for example, complete captured records elements, documented and maintained metadata, document management, and access. Metadata, for example, records metadata and the system is documented and accessible, there are regular metadata updates. Use and records systems, for example, consistency and recovery period, access management, access security. Usability maintenance, for example, metadata can be accessed anytime, authenticity and integrity, retention, hardware, and software management. Depreciation, for example, documented and authorized depreciation, procedures, documented and authorized destruction. A summary of the risk sources for the processes can be seen in Figure 5, below.

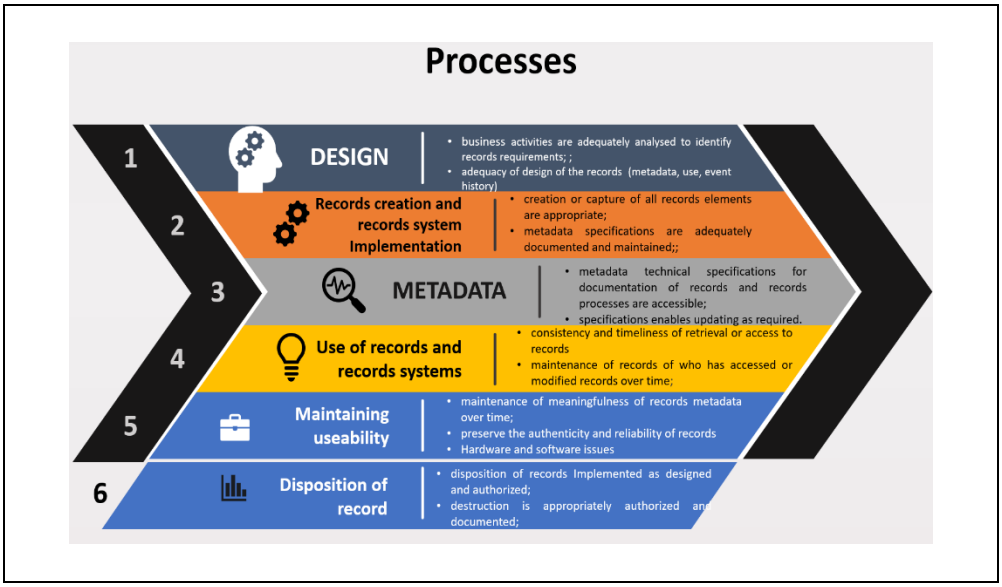

Figure 2. Areas of uncertainty: Processes
(Source: adapted from (ISO 2014)

When risk identification is successfully carried out by inspecting these areas of uncertainty, the next step is to analyze these risks. The analysis is carried out by classifying these risks by adding value. The activity of assigning this score is done by calculating the frequency of events, then assigning a number (score) to make it easier and clearer. The scores categories commonly used are:

1) very rare (occurs once in 10 years);
2) rare (occurs once every 3 years);
3) frequent (occurs once a year);
4) very frequent (occurs more than once per month).

After conducting the analysis, then an evaluation is carried out by categorizing it based on the impact that will appear when the risk occurs and not properly addressed. The scale of the impact is usually small, medium, large, and severe. The illustration of the application of the impact scale can be seen in Table 3 below.

Table 3 Example of classification of impact assessment of adverse events

Minor	Moderate	Major	Severe
Anomalous breach of access	Unauthorised access to records	Unauthorised access to records –	Widespread loss, unauthorized

Minor	Moderate	Major	Severe
restriction;		shall be reported	access and damage
Damage to small quantity of records in one area of operations	Damage to significant quantity of records in one area of operations	Damage to core records of operations spreading to several areas	Damage to core records in majority of areas of operations
Limited loss of data	Loss of data/damage to reliability	Loss of data/damage to reliability; damage to reputation	Loss of data/lost of reliability/loss of public trust
Recoverable loss	Operations not disrupted; records recoverable with effort	Loss admitted; disruption to more than one area of operations; recovery effort costly	Operations shut down; recovery effort costly and time-consuming; records not recoverable

Source: (ISO 2014)

Prediction or calculation impact is critical because from these results the priority level is determined. The mitigation actions taken depend on the impact level, the smaller mitigation actions needs, the risks could be negligible, or it is enough just to know and documented the risk without any treatment. Conversely, when the impact is severe, the mitigation actions taken are also large and must be predictable and planned, including who will take responsibility to handle it.

Figure 3. Risk Management Cycle
(Source: researcher data finding)

Based on the previous description, the risk detection mechanism is part of risk management. This process runs circularly from risk identification, analysis through value determination, evaluation through impact determination, and then mitigation actions that must be taken. Risk detection in digital information management from the perspective of records management is part of an organization's broad risk management framework.

4. CONCLUSION

Based on the analysis, it can be concluded that in the context of e-government in Indonesia, the risk detection framework in line with records management perspective as formulating in ISO / TR 1828 is very compatible and relevant to apply to manage the digital information. Because it comprehensively highlights risks in these aspects, context (external and internal), records systems, and also the records processes. However, the success rate of implementing this framework in the field depends on the extent to which the records management perspective or paradigm reform from non-digital to digital within the government agencies occurrence.

REFERENCES

Anderson, K. (2015). "Building Trust and Confidence through Sustainable Information Systems Research: Towards a Common Future." In *5th International Conference The Future of Information Sciences*, 9–15. Zagreb: University of Zagreb. https://core.ac.uk/download/pdf/299373057.pdf.

ANRI. (2011). "Pedoman Penyelenggaraan Kearsipan Di Lingkungan Perguruan Tinggi."

Bawono, H. (2017). "Simplifikasi Ke-Arsip-an (Elektronik): Akar Terseoknya Kearsipan Indonesia Dalam Belantara E-Government." In *Diskursus Kearsipan Indonesia: Sebuah Bunga Rampai*, 1–76. Depok: RajaGrafindo Persada.

Bearman, D. (1993). "Record-Keeping Systems." *Archivaria* 36 (Autumn 1993): 16–36. https://archivaria.ca/index.php/archivaria/article/view/11932/12886.

Berner, J. S., & Boel. (2003). "Constructing Risk and Safety in Technological Practice: An Introduction." In *Constructing Risk and Safety in Technological Practice*. London: Routledge.

Borglund, E. (2006). "A Predictive Model for Attaining Quality in Recordkeeping." Mid Sweden University.

BPKP. (2018). "Pedoman Pengawasan Intern Berbasis Risiko."

Cook, T. (2007). "Electronic Records , Paper Minds : The Revolution in Information Management and Archives in the Post-Custodial." *Archives & Social Studies: A Journal of Interdisciplinary Research* 1 (0): 399–443. https://pdfs.semanticscholar.org/815d/a1b4f15de9611accdf364d72df74024e527b.pdf.

CRMSIndonesia. (2019). "Survei Nasional Manajemen Risiko 2019." Jakarta. https://crmsindonesia.org/wp-content/uploads/2019/11/CRMS-Indonesia-Survei-Nasional-Manajemen-Risiko-2019.pdf.

Duranti, L. (2001). "Concepts , Principles , and Methods for the Management of Electronic Records." *The Information Society* 17 (4): 271–79. https://doi.org/10.1080/01972401753330869.

Duranti, L., & Blanchette, J. (2004). "The Authenticity of Electronic Records : The InterPARES Approach." Vancouver.

Egbuji, A. (1999). "Risk Management of Organisational Records." *Records Management Journal* 9 (2): 93–116.

IronMountain. (2015). "A PRACTICAL GUIDE FOR A RECORDS AND INFORMATION MANAGEMENT RISK & CONTROL FRAMEWORK." Boston.

ISO. (2014). "ISO/TR 18128 Concerning Risk Assessment for Records Processes and Systems." Switzerland: ISO.

ISO. 2016. "ISO 15489-1:2016 Information and Documentation-Records Management-Part 1: Concepts and Principles." Geneva: ISO.

Katuu, S. (2012). "Enterprise Content Management (ECM) Implementation in South Africa." *Records Management Journal* 22 (1): 37–56. https://doi.org/10.1108/09565691211222081.

Katuu, S. (2016). "Managing Digital Records in a Global Environment: A Review of the Landscape of International Standards and Good Practice Guidelines." *The Electronic Library* 34 (5): 869–94. https://doi.org/10.1108/EL-04-2015-0064.

KemenPANRB. (2019). "SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)."

PARBICA. (2004). "GUIDELINE 18: Digital Preservation."

Rogers, C. (2015). "Authenticity of Digital Records in Practice." In *2015 Digital Heritage*, 7–10. Granada: IEEE. https://doi.org/10.1109/DigitalHeritage.2015.7419532.

Woodal, A. B., & Philip, J. W. (2014). *Total Information Risk Management: Maximizing the Value of Data*. Massachuset: Elsevier.

Informant A, Interview by Harry Bawono. (2019). Electronic Records Management in ExxonMobil (April 8-12).

Informant N, Interview by Harry Bawono. (2019). Risk Management Frameworks in Government Agencies (May 23).

Informant F, Interview by Harry Bawono. (2019). Risk Management and Information Security (November 5).