Bilgi Yönetimi Dergisi

Cilt: 5 Sayı: 1 Yıl: 2022

https://dergipark.org.tr/tr/pub/by

Peer-Reviewed Articles
Research Article

Article Info

Date submitted: 04.05.2021
Date accepted: 09.07.2021
Date early view: 25.04.2022
Date published: 30.06.2022

Makale Bilgisi

Gönderildiği tarih: 04.05.2021
Kabul tarihi: 09.07.2021
Erken görünüm: 25.04.2022
Yayınlanma tarihi: 30.06.2022

Keywords

Digital Continuity, Information Management, Born-Digital Records

Anahtar sözcükler

Dijital Süreklilik, Bilgi Yönetimi, Doğuştan Dijital Belge

DOI numarası

10.33721/by.932771

ORCID

0000-0003-0474-3584 (1)

0000-0003-3841-3751 (2)

Belediyelerde Dijital Süreklilik Uygulamaları: İstanbul'daki Belediyeler Üzerine Bir İnceleme

Digital Continuity Practices in Municipalities: A Study on Municipalities in Istanbul

Lale ÖZDEMİR ŞAHİN
Bartın Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğretim Üyesi,
lsahin@bartin.edu.tr

Varol SAYDAM
Marmara Üniversitesi Bilgi ve Belge Yönetimi Bölümü Araştırma Görevlisi,
varol.saydam@marmara.edu.tr

Abstract

The development of information technologies and the creation of applications has ensured that access to corporate information and records can be achieved independently of time and place. However, the digital continuity of digital information is at risk because the above transformation is sometimes not carried in conjunction with the necessary policies. This paper examines the degree to which digital continuity is practised and embedded across municipalities in Istanbul, and aims to determine their digital continuity risk exposure. Digital continuity relates to the ability to access and use digital information for as long as is necessary for business activities. Crucially, digital information created by organisations in the course of their business activities should be trustworthy. Digital continuity is not just about technology, it is about an organisation ensuring that it has the right policies and practices in place for the management of born-digital information so that it remains usable over time. The digital age has rendered the management of information more complicated especially given that digital information is more vulnerable, and within this framework, this study aims to survey municipalities on the topic of awareness of digital continuity practices. This study determines the extent to which a sample of Istanbul-based municipalities are aware of and embed digital continuity practices in their organisations. This study concludes that although awareness of digital continuity is evident, that practice is still lacking in some areas.

Öz

Bilgi teknolojilerinden gelişimiyle birlikte üretilen uygulamalar, kurumsal bilgi ve belgelere zaman ve mekandan bağımsız erişim imkanı sağlamıştır. Ancak, gerekli politikalar çerçevesinde yürütülmeyen bu değişim, dijital sürekliliği tehdit etmektedir. Bu çalışma, dijital sürekliliğin belediyelerde ne ölçüde benimsendiğini ve uygulandığını incelemekte ve belediyelerin dijital süreklilik konusunda karşılaşabilecekleri riskleri belirlemeyi amaçlamaktadır. Bu çerçevede, dijital süreklilik uygulamaları konusunda belediyelerin farkındalığını araştırılacaktır. Araştırma İstanbul'daki belediyelerle sınırlandırılmıştır. Dijital süreklilik, kurumun faaliyetleri çerçevesinde ihtiyaç duyulduğu sürece dijital bilgiye erişme ve kullanma yeteneğiyle/kapasitesiyle ilgilidir. Bu noktada, kurumların faaliyetleri sırasında ürettikleri dijital belgelerin güvenilir ve öznitelikleri korunmuş halde erişilebilir olması gereklidir. Dijital süreklilik, sadece teknolojiyle değil, kurumun dijital ortamda üretilen belgelerinin yönetimi ile doğru politika ve uygulamaları sağlamasıyla ilgilidir. Bu sayede dijital bilgiler zaman içinde kullanılabilir. Belediyelerde gerçekleştirilen anket çalışmasıyla, belediyelerin dijital süreklilik uygulamalarından ne ölçüde haberdar oldukları ve kurumlarını bu süreçlere ne ölçüde dâhil ettikleri incelenmiştir. Çalışmanın sonucunda, dijital süreklilik farkındalığı olmasına rağmen, bu konudaki uygulamaların bazı alanlarda hala eksik olduğu sonucuna varılmıştır.

** The research and publication process of this article was carried out in accordance with "Research and Publication Ethics".*

1. Introduction

Information is a critical asset for the provision of services to the public and for the effective management of municipalities, services and resources. Information assets that are digital, as opposed to, analog, are by nature more vulnerable, voluminous and diverse, and should not be managed like paper records. This is because digital information is not static, and its trustworthiness over time cannot be guaranteed. In recent research by Moss et al., it is argued that it is delusional to imagine that any kind of order can be imposed on all but a fraction of digital content even at the time of creation, and that even the application of metadata to digital records is not as helpful or as straightforward as it may seem (2018, p. 2, 6). As daunting the prognosis by Moss et al. may be, the current reality in Turkey is that records are managed with order imposed, mainly, within electronic records management systems.

This article reviews the awareness and implementation of digital continuity across municipalities in Istanbul, Turkey. The study aims to examine the digital continuity risk exposure through taking a representative sample of Istanbul based municipalities. Digital continuity relates to the ability to access and use digital information for as long as is required by organisations. The implementation of digital continuity is only possible if an organisation manages its information as valuable assets. Local authorities or municipalities make up local government and are responsible for providing frontline services to their citizens, and at the same time, are accountable to central government. A study carried out in 2000 highlighted the view that local government officials argued that municipalities should be able to transfer their records to local places of deposit rather than the Turkish State Archives (İcimsoy, 2000, p. 61). However, despite the fact that local authorities possess some autonomy administratively and financially from central government, this does not exempt them from being legally bound, like any other public sector organisation, to manage records electronically, and to transfer records selected for permanent preservation to the Turkish State Archives. In anticipation of the implementation of information management systems, municipalities were legally bound to adopt classification schemes for the management of their electronic records in 2005. This was prior to the use of information management systems becoming compulsory in 2008. In his 2008 study, Çiçek highlighted the issues faced by municipalities in adhering to a national classification scheme that was at times difficult to align with municipality-specific functions (Çiçek, 2008, p. 495-498). Municipalities have been implementing electronic records management for over a decade, which renders the examination of how far digital continuity is embedded across municipalities in Istanbul both logical and necessary.

Istanbul, the most populated province of the Turkish Republic has forty municipalities (also known as local authorities), thirty-nine of which are district municipalities, and the Istanbul Metropolitan Municipality which has been in existence since 1984. A two-tier municipal system exists in much of Turkey, with legal powers given to both district municipalities and the metropolitan municipality in the same jurisdiction (Union of Municipalities of Turkey, n.d.).The Istanbul Metropolitan Municipality has jurisdiction over 5460,85 km and oversees the provision of local government services. The strategic responsibilities of local municipalities in Istanbul include the following: general management, which (also includes information technologies, document and archival management), disaster management, local planning, environmental planning, health services, social support and cultural services management (Fatih Belediyesi, Stratejik Plan, 2021, p. 31). In terms of the most basic provision of service, citizens expect their municipalities to collect their refuse, neuter local stray animals, and to ensure that local town planning of neighbourhoods is carried out in a timely and efficient manner. Municipalities are legally obliged to serve their communities whilst enforcing wide-ranging local and state laws. The management of digital information as an asset within the framework of risk management will mean that municipalities will be able to ensure that the continuity of their information becomes a reality. This will in turn have a direct and positive impact on the continuity of services, which includes e-services, offered to communities- all of which require the use and management of information assets.

The existence of robust and effective information practices in municipalities is vital if information governance is to be implemented properly. The existence of information governance in any given organisation means that information assets held by organisations are managed within the framework of risk management, and in a transparent, and accountable manner. More specifically within the context of local government and municipalities as organisations, information governance can be defined as the following; as a term that is used to describe the way legal requirements are managed, and ensures that

both business and personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible services (Coventry City Council, 2021). Another definition of information governance is closely related to that of recordkeeping, and "is concerned with how information is held, obtained, recorded, used and shared" (Nottinghamshire County Council, 2018). For the purpose of this study, the definition of information governance used by the National Archives of Australia will be employed; information governance is a system for managing information assets across an entire organisation to support its corporate outcomes (National Archives of Australia, 2021).

2. Digital Continuity

The term 'digital continuity' was coined by the UK National Archives to mean establishing an ability to access and use digital information for as long as needed by organisations through organisational, business and technology changes (The National Archives, 2010, p. 8). Digital continuity is not completely synonymous with digital preservation. According to the Digital Preservation Coalition, digital preservation refers to the series of managed activities necessary to ensure continued access to digital materials for as long as necessary. Digital preservation also refers to all of the actions required to maintain access to digital materials beyond the limits of media failure or technological and organisational change (Digital Preservation Handbook, Glossary, 2021). Whereas, digital continuity is concerned with the ability of digital information being usable for as long as required through change that can render digital information vulnerable, such as technological, organisational and operational change. To put it simply, digital preservation primarily focuses on long term preservation whereas the emphasis for digital continuity is on business need. Digital continuity refers to the usability of information. According to the UK National Archives, digital information is useable if it can be found when needed, it can be opened as needed, it can be worked with in the way needed, it can be understood, and it can be trusted.

2.1. Digital Continuity as Risk Management

An understanding of the term 'digital continuity' in its own right distinct from established electronic information management practices in Turkey is not widespread. There is a lack of awareness of how digital continuity is more than just ensuring that information is managed properly for evidential purposes. The definition of information management as "principles and techniques to process, store, retrieve, manipulate, and control access to information so that users can find information they need" (Pearce-Moses, 2005, p. 204) is one that runs parallel with that of digital continuity because of the emphasis on access and usability. However, digital continuity is ultimately about the risk management element of digital information.

Managing digital continuity protects the information that organisations rely on to do business. This applies to all organisations regardless of size and whether they operate in the public or private sector. In the case of municipalities, implementing digital continuity means that they can operate accountably, legally, effectively and efficiently. If digital information remains useable and trustworthy over time then it helps to protect municipalities' reputation, which can result in informed decisions, cost reduction, and better public services. If information is lost or unfindable because digital continuity isn't managed properly, the consequences can be as serious as those of any other information loss (The National Archives, n.d.). The lack of digital continuity in municipalities could result in scenarios such as the following:

- Delays in the legal process on the regeneration of neighbourhoods because digital information cannot be found
- Applications by disadvantaged members of the community for benefits are lost after the implementation of new technology
- Data required for natural disaster planning is buried in out of-date software
- Sensitive information is inadvertently shared externally because it was not on the information asset register.

Organisations and, for the purposes of this study, municipalities are most at risk when gaps exist in information governance structures. Information management policies and practice are insufficient if change management, technology management and information management processes are not properly integrated (The National Archives, 2017b, p. 7). This means that a municipality's information can be at risk if it undergoes change management when there is a change in senior management due to local elections, or when a new information management system is implemented across a municipality. Information can also be at risk if data is not migrated successfully between systems, thus resulting in the loss of metadata.

2.2. How to Implement Digital Continuity

It is argued that municipalities should implement digital continuity practices, but in reality what does this actually mean? The first requirement is that information should be treated as an asset, and that all municipalities should keep and regularly review their information asset registers. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently (The National Archives, 2017a, p. 1). This would equate to digital information being managed from the point of creation, and any metadata recorded would allow for risk-based decisions to be made; such as whether the information can be shared, internally and externally, file path, sensitivities of the information, file format and retention period. Another important step in putting digital continuity on the agenda of senior management in organisations, is to appoint a Senior Responsible Owner (SRO) for digital continuity at a senior level. This responsibility can also be given to Chief Information Officers (CIO). In addition, every business unit should have an Information Asset Owner, who is familiar with the nature and content of the information created and used in that business unit. Also, a multi-disciplinary team should be established to take action on managing digital continuity, which includes skills from Information Management and Information Technology (IT). This is to ensure that a holistic approach is taken to digital continuity, and the emphasis should be on a risk-based approach to protecting information rather than just on the use of technology. Ultimately, a municipality should know the technical environment where information is stored, what its information assets are, and its business needs (The National Archives, n.d.).

Municipalities should define their digital continuity requirements and the risks associated with their digital information, and devise a plan of action. For example, if staff are unclear on their responsibilities for managing information, loss of digital continuity is not acknowledged as an important corporate information risk, or if IT service providers are not aware of their responsibilities, then an action plan has to be put into place (The National Archives, 2017b, p. 17). One of the key aims of digital continuity is to mitigate risk as is illustrated in the above examples. If information is stored in proprietary formats or the general rule to retention is to retain records indefinitely, then action should be taken by municipalities to mitigate the risks that will arise from inadequate information management practice.

3. Information Management in Municipalities

3.1. E-Information Services in Municipalities

Municipalities have a varied remit and operate in accordance with both the Municipality Law (No. 5393) and the Metropolitan Municipality Law in Turkey (No. 5216). The Municipality Law stipulates that municipalities have a responsibility, among other things, to undertake regeneration, canalisation and water works, in addition to building urban transport infrastructures and implementing environmental health regulations. Municipalities also have responsibility for local law enforcement, emergency services, marriage and burial services, culture and the arts. Municipalities that have a population of more than fifty thousand are also obliged to open shelters for the vulnerable (Belediye Kanunu, Madde 14(a)).

The proliferation of internet technologies resulted in the provision of communication technologies services becoming easier, cheaper, faster, more transparent and reliable. This in conjunction with increased participation by citizens, resulted in the development of policies on electronic communications and open government (Pektaş, 2011, p. 69). Global advances in technology ensured that public sector bodies were compelled to make changes to their functions, including to their economic, technological, social and cultural infrastructures. The benefits of the use of technology in everyday life resulted in the

diversification of the public services provided by local government. Public services in Turkey were made available online within the framework of the concepts of e-Government and e-municipality, and the implementation of locally based services was referred to as e-municipality (Erdoğan, 2019, p. 552). Information in the e-Government portal services are either of an informative nature or are transaction-based. Through the e-municipality gateway, information on daily civil wedding schedules, local assembly and council proceedings, the current market value of plots and real estate, as well as dilapidations surveys, environmental tax dues, and licensing can be accessed (Sağlık, 2015, p. 4, 72-73). Whereas transactions that can be carried out online are usually those born out of a legal requirement. Such transactions include the payment of taxes or dues for environmental tax, advertising fees and housing tax. Non-financial transactional services that can be carried out via e-municipality include making reservations at cultural centres, purchasing tickets for arts functions, registering pets with the municipality veterinary and applying for municipality run educational courses (Sağlık, 2015, p. 75-76).

The provision of e-Municipality services was primarily made possible through the use of information management systems becoming widespread across municipalities and through the development of the e-Government infrastructure. In today's Turkey, municipalities perform the majority of their services electronically; data is generated on carpark usage, the monitoring of local law enforcement, local transport services, and the voluminous applications made by citizens for services. As discussed below, municipalities are not exempt from transferring records worthy of permanent preservation to the archives, which renders the implementation of digital continuity even more important.

3.2. Information Management Practices in Municipalities

In accordance with the Turkish Archival Services Regulations, public bodies are required to transfer their records to the state archives once they reach their transfer date at either 20 or 15 years old (Devlet Hizmetleri Hakkında Yönetmelik, 2019). Municipalities are also subject to the regulations and like other public bodies, have to ensure that their records remain readable, usable and trustworthy until they transfer those selected for permanent preservation to the archives. The focus of corporate electronic records management in Turkey is within the framework of the use of EDRMS, and with the implementation of the Prime Ministerial Circular in 2005, municipalities had to adhere to a standard file plan for their EDRMS. The Turkish Standard (TSE) TS 13298 on Electronic Records Management also became compulsory, which witnessed municipalities not only having to work within the parameters of a centrally devised file plan, but also having to follow a national standard on the creation and management of electronic records. The Turkish standard has been revised twice since its publication in 2007, and was made compulsory for the public sector in 2008. The 2015 version of the standard includes an emphasis on archival management and provides a regulatory framework for sharing information between organisations, the use of secure e-mail, and corporate archiving (TS 13298, 2015). Digital transformation in Turkey began a few years before the implementation of the first version of the standard on electronic records management in 2007.

The e-Transformation initiative in Turkey began in 2003 and aimed to offer citizens a more transparent, better quality and effective public service that resulted in the publication of the Interoperability Principles. Interoperability is defined as "the ability of a system or process to use the information or functionality of another system or process based on common standards" (DPT, 2005, p. 5). As discussed later, these principles are of great significance to the success of offering public services via the digital e-Government platform, because they stress the need for corporate processes to be integrated, transparent and simplified. All public bodies, including municipalities, had to adhere to the Interoperability Principles by ensuring that their information management systems met the requirements of the principles (Resmi Gazete, 25897). The Interoperability Principles Guide was revised in 2009 and again in 2012 to take account of the changing needs of public bodies. The topics covered by the guide aimed to increase the effectiveness of the e-Government gateway in the provision of public services through creating the foundation of interoperability between public bodies by rendering easier back-office integration (Birlikte Çalışabilirlik Esasları Rehberi, 2009)

Governance also extended to the use of e-mail; the e-Correspondence Project was launched under the coordination of the Digital Transformation Office with the aim of ensuring that official correspondence between public sector organisations was carried out in a secure electronic environment. It became

compulsory for public bodies to implement the e-Correspondence technical guide, and they were able to use Application Programming Interface to integrate corporate e-mail to information management systems. Most recently, as a result of the revised Official Correspondence Regulations, public bodies can only create a single copy of a digital record (Resmî Yazışma Yönetmeliği, 2020). This is an essential practice, as it deters records from being signed and managed in a physical environment, and goes a long way to reduce unnecessary digital duplicates.

4. Methodology and Data Sample

This study is of a valuable nature because municipality's information can be at risk if it undergoes change management when there is a change in senior management due to local elections, or when a new information management system is implemented across a municipality. Information can also be at risk if data is not migrated successfully between systems, thus resulting in the loss of metadata. Given that the above changes can apply to any of the municipalities in not only Istanbul, but Turkey also, increases the originality of the current research. This study reports on research carried out between 2017-2020 on municipalities in Istanbul. This study employed descriptive research methods and survey which aimed to gain an insight into the awareness of digital continuity practices. Marmara University Social Sciences Ethics Committee has unanimously decided that this research is ethically appropriate at its meeting dated 05.01.2022 and numbered 2021-139. Surveys were sent electronically to every municipality in Istanbul, including the Istanbul Metropolitan Municipality. The survey method was used to increase the likelihood of securing responses because the survey clearly stated that responses would be anonymous and that the names of municipalities would not be required for the purposes of the study. This decision was taken in order to encourage frank and honest answers from respondents. In the way of limitations, it has taken a lengthy period of time to gain sufficient data to draw some worthwhile conclusions, and the survey had to be sent out on a few occasions before a sufficient number of responses were received. Also, it is a well-known drawback of using surveys as a research method that respondents wish to show their authority in a favourable light (The National Archives, 2010, p. 8). Given the above limitations, this study can be considered to be a snapshot into the awareness of digital continuity across municipalities in Istanbul, rather than a definitive and static portrait of current digital continuity practices. This is especially true given that the anonymous nature of the data allows insights into digital continuity practices generally across Istanbul, without pinpointing the progress, or lack of, at specific municipalities. This study is unique as it is the first of its kind to focus on the implementation of digital continuity across municipalities.

The primary source of data for this study is an electronic survey sent to municipalities in Istanbul. The survey was also made available on a public forum of the Union of Municipalities of Turkey. The survey was aimed at information professionals and a total of 27 responses from different municipalities were recorded. The survey comprised of a total of 11 questions, 8 closed-ended and 3 open-ended, which allowed for respondents to provide any additional information they deemed to be relevant. The survey contained a brief definition of digital continuity as follows; "digital continuity can be defined as the ability to use and access information created in an electronic environment for business purposes for as long as required and in the way required." The survey questions are as follows:

(1) Does your organisation use an electronic records management system (ERMS)?

(2) Which department is responsible for records management and ERMS?

(3) With the exception of ERMS does your organisation use any other systems or save information on any other digital platforms?

(4) Does your organisation keep an information assets register?

(5) Does your organisation have a Chief Information Officer (CIO)? If not, who has the responsibility for information management?

(6) What are the reasons for issues relating to information access?

(7) Does your organisation have a digital continuity policy?

(8) Does your organisation have a policy on data migration?

(9) Does your organisation have a policy on file formats?

(10) Do you think that municipalities should provide in-house training on digital continuity?

(11) Which public body do you think should be responsible for formulating policy on digital continuity?

The survey received 27 responses from different municipalities, and although this sample does not constitute a response from all Istanbul municipalities, the data provided is nonetheless sufficient to gain an insight into whether digital information is managed with continuity in mind. In addition to the data obtained from the survey findings, the Scoping Report to The National Archives on the Local Government Digital Continuity Requirement is also used as a source for this study (The National Archives, 2010). Even though the report mentioned above was based on municipalities in the United Kingdom, and was published in 2010, does not diminish its significance for the present study. Even though the findings from the Scoping Report date from 2010, the continuing validity of the data still exists. It is argued for the purpose of this study that the data from the aforementioned report is comparable to the findings of the current study because the implementation of electronic records management systems in the United Kingdom began earlier from 2003 onwards, earlier than implementation in Turkey. Thus, the United Kingdom public sector had been implementing EDMS for seven years by the time the Scoping Report was published. The aim of the report is also parallel to the current study: "to analyse the digital continuity risk exposure through taking a representative sample of principal local authorities." (The National Archives, 2010, p. 2). Indeed, the data obtained from the current survey can be said to be more representative of the sample population than the data obtained for the Scoping Report. This is because a response rate of only 30 per cent was achieved by the 2010 study (The National Archives, 2010, p. 2) whereas a 67 per cent response rate (twenty-seven municipalities) was achieved for the current study. The survey findings have been compared, where relevant, with the findings of the scoping report in order to determine whether the issues faced by municipalities with regard to digital continuity in the United Kingdom are comparable to those faced by municipalities.

5. Findings

5.1. Use of ERMS in Municipalities

In relation to the first survey question, which asked whether municipalities used electronic records management systems, 25 of the 27 respondents stated that the municipality they worked in used an ERMS. Of the remaining two respondents, one stated that an ERMS was not used, and the remaining respondent stated that ERMS implementation was at planning stage. The data obtained from the survey results on this question is not at all surprising given the lapse in time since the early 2000s, which witnessed the beginning of electronic records management in Turkey.

By 2007, most public sector organisations were actively implementing electronic records management. According to Kandur, this trend can be attributed to standards which were developed in 2007 for managing electronic records. These standards were subsequently rendered compulsory for the public sector in a circular issued by the Prime Minister's Office in 2008 (Kandur, 2016, p. 527). The high rate of ERMS implementation across municipalities in Istanbul is certainly significant. However, given that municipalities offer a wide-range of services across e-Government platforms, including services relating to town planning, tax payment and licensing, it is crucial that the systems used can integrate with other systems to ensure a continuity of service (Özdemirci, 2016). The implementation of an electronic records management system is only the beginning of the long journey to ensuring digital continuity. The Scoping Report, which examined digital continuity risk across UK local authorities found that by 2010, over two-thirds of those responding to the questionnaire said an EDRMS was in use, or was at development stage. In many local authorities an EDRMS was only used in some of the organisation (The National Archives, 2010, p. 14). According to the survey results of the current study, the rate of EDRMS/EDMS implementation is higher across municipalities in Istanbul compared to implementation across UK local authorities.

Table 1

Responsibility for Records Management and ERMS

Which department is responsible for records management and ERMS?	No. of municipalities
IT Directorates/departments	16
Administrative Affairs Directorates	4
IT, Strategic Development and Administrative Affairs Directorates	2
IT and Administrative Affairs Directorates	3
IT Directorate and Archives Department	1
Directorate for Strategic Development	1
Total	**27**

The second survey question aimed to determine where the responsibility for records management and ERMS lay within municipalities. As can be ascertained from Figure 1, over half of respondents stated that IT Directorates/departments were solely responsible for the oversight of records management and ERMS. Other divisions or directorates that have responsibility for records management and ERMS include Administrative Affairs Directorates and the Directorate for Strategic Development. In some municipalities, the responsibility for records management and ERMS was shared between directorates, such as between IT and Administrative Affairs Directorates, and between the IT Directorate and Archives Department. In two municipalities, the responsibility was shared between three directorates; IT, Strategic Development and the Administrative Affairs Directorate. According to Adam, who was responsible for the implementation of an ERMS at a local authority in southeast England, the technical aspect of ERMS was the easiest part, whereas ensuring cultural change was far from easy; "It's more about people, organizations, organizational culture, change, cultural change, managing cultural change, and good, strong, yet flexible project management." (Adam, 2008, p. 18-19). The implementation of an ERMS/EDRMS is not just about technology. It is about information governance, recordkeeping and information management. The municipalities in Istanbul that share responsibility for ERMS and records management are on the right track as ERMS is not the domain of one department or directorate. It is ironic that records management departments or divisions are not named as being involved in the responsibility for ERMS, thus highlighting the low profile of records management in municipalities.

In order for digital continuity risk exposure to be minimalised, staff from across different departments have to be involved. Each department should have clearly defined roles and responsibilities on digital continuity. Ideally, even if IT has overall responsibility for ERMS, which appears to be the case in many Istanbul municipalities, each department should have its own ERMS champion who also acts as Information Asset Owner. This is because it is the creators and users of information assets that are most likely to understand the content, context and importance of them.

Table 2

Other Digital Platforms

With the exception of ERMS does your organisation use any other systems or save information on any other digital platforms?	No. of municipalities
Yes (No information provided)	1
No	6
Digital Archive	11
Server	5
Shared Drive	2
Storage	1
Active Domain	1
Total	**27**

The third survey question asked municipalities the following, with the exception of ERMS, does your organisation use any other systems or save information on any other digital platforms? Given that municipalities offer a range of services across various digital platforms, it is to be expected that several municipalities stated that they used other digital platforms and systems apart from ERMS (21 municipalities). Figure 2 contains the answers provided by information professionals in municipalities, and 11 of the 27 respondents stated that their municipality used digital archives, in addition to ERMS. However, the use of digital archives is concerned more with performing corporate functions and storing digitalised documents rather than with the long-term preservation of records. In relation to this question, one of the respondents answered as follows; "different systems are used for both the town planning and licencing archives. File formats such as TIFF, JPEG and PNG are used. Other records are captured in ERMS." Another respondent highlighted the fact that records management practices differed among municipalities; "for the present time our archives are being migrated one by one to the ERMS. Digital archives from seven directorates have been migrated to ERMS." This example is another illustration of how digital archives in municipalities are not archives in the traditional sense of the term, but more modules used to manage the e-services provided to the public. On this topic, the Scoping Report found that:

"Much of the information captured and stored by local authorities relates directly to the services they provide. Many of these services are supported by "line of business" applications which combine structured databases linked to unstructured documentation (letters, forms etc.). When these systems are replaced, a proportion of the data will be migrated to the new system." (The National Archives, 2010, p. 13).

The use of various digital systems in municipalities to carry out the services they provide and the integration between systems is a positive development, as long as the information assets in those systems are managed properly. The survey findings also showed that some municipalities still use shared drives in which to store information. This is, of course, not a sound practice as it increases digital continuity risk because shared drives do not provide sufficient access controls, and it is difficult over time to locate information, thereby posing a risk to information governance. Indeed, a study on municipalities stressed the need for municipalities to manage efficiently the change and transformation brought about by technological developments, otherwise they would come face to face with the loss of their corporate memory (Akdoğan et al., 2016, p. 211).

5.2. Information as an Asset

The fourth survey question asked municipalities whether an Information Asset Register was used, and 16 municipalities in Istanbul stated that they did use Information Asset Registers. This figure constitutes almost 60 per cent of respondents. The use of Information Asset Registers is critical if digital continuity risk is to be managed. A municipality cannot use its digital information for as long as required, and in the way it wishes to, if the assets that comprise of information are not managed. For example, if documents and plans of a local regeneration project are not managed as a single asset, then risks associated not only with accessibility but also sensitivity and disposal will increase over time.

Although it is not impossible that 60 per cent of Istanbul based municipalities keep an Information Asset Register for digital information, it is a possibility that some of the respondents answered the question with information security assets in mind. This is because most municipalities have information security accreditation in line with the international standard ISO 27001, therefore they may associate the information asset register they maintain with information security assets such as employee laptops, encryption keys or databases. Whilst not necessarily incorrect, as databases and laptops ultimately contain information, they are nonetheless technology assets. It is the information within the technical environment which is classed as an information asset from the perspective of digital continuity. The Scoping Report which, was carried out on UK local authorities, found that many municipalities outsourced their IT, but none of the respondents stated that the outsourcing partner was definitely obliged to maintain an Information Asset Register (The National Archives, 2010, p. 14). Thus increasing the risk of a local authority incurring financial or reputational damage. The Scoping Report also recommended that the use of methods to put an indicator of business value on information assets in local authorities be encouraged so that this could help inform digital continuity processes and decisions (The

National Archives, 2010, p. 3). In order to limit risk exposure municipalities should ensure that all third party suppliers are obliged to keep and regularly review an information asset register.

5.3. Chief Information Officers and Responsibility for Information Management

The fifth survey question was as follows: Does your organisation have a Chief Information Officer (CIO)? If not, who has the responsibility for information management? Effective management of digital continuity includes defining roles and responsibilities. According to the survey data, almost 45 per cent of municipalities have a CIO which is a positive development in terms of information being treated as an asset and defining roles on information management and digital continuity. It is logical that the CIO of an organisation would also be appointed Senior Risk Officer (SRO) for digital continuity. Without clearly defined roles, staff and suppliers will not have a full understanding of what is expected of them, will lack accountability, and be unable to ensure continuity of the information assets for which they are responsible (The National Archives, 2017b, p. 17).

Table 3

Responsibility for Information Management

Responsibility for information management	**No. of municipalities**
IT Directorate	9
I don't know/non applicable	4
'Management'	1
Strategic Development	1
Total	**15**

As can be ascertained from Figure 3, the 15 respondents who did not have a CIO at their municipality answered the second part of the above question on information management responsibility. The majority of respondents stated that IT directorates are responsible for information management, and this stems from the fact that IT directorates run and manage Information management systems such as ERMS. This can be viewed as positive because information management controls are in place. However, the Scoping Report's findings err on the side of caution and warn that information practices should not be viewed within the context of ERMS:

"A noticeable trend from the survey results was that information management controls, such as developing a classification scheme or file plan appear to be related to the introduction of an Electronic Document and Records Management System (EDRMS). Whilst any information management improvements are welcome, it is worrying that they are so often driven by a single technology or environment. Tools such as classification schemes are abstractions of business activities and of wider use in business management and transformation than purely within EDRMS" (The National Archives, 2010, p. 14).

The warning in the above quote can be said to apply not just to municipalities, but to other public sector organisations in Turkey. It is telling that a significant number of municipalities, and other organisations, use ERMS/EDRMS but they do not have a published information management policy or a records management policy in place. Çiçek in his recent study draws attention to the fact that records management policies are the exception rather than the norm for Turkish organisations (Çiçek, 2020, p. 397). Technology is only one dimension of digital continuity, and information risk cannot be managed successfully without policies in place, because it is policies that generate accountability, responsibility and transparency.

Table 4

Information Access Issues

Information Access issues	
File format issues	8
Lack of leadership regarding information management	2
Ineffective migration of information to new Technologies	9
No information access issues	14
*some respondents chose more than one answer	2
Total	**35**

The sixth question asked about information access issues. As can be seen from Figure 4, respondents chose from the following answers: file format issues, lack of leadership regarding information management, ineffective migration of information to new technologies and no information access issues. According to the survey data, 52 per cent of respondents stated that there were no information access issues within their organisation. This is a significant finding for the purposes of the current study as accessibility is an important component of digital continuity; being able to find and use information when required. Despite this, the next most popular answer relates to issues with the ineffective migration of information to new technologies at 33 per cent. The implementation of information management systems in most municipalities has occurred over the last decade and this finding illustrates that post-implementation migration difficulties arise between new and legacy technologies. The above increases digital continuity risk exposure, and this finding is echoed by the Scoping Report, which found that migration of information was primarily driven by financial factors with old systems also kept running in parallel to provide access to old data. It was even noted that in one case information was held on a COLD (Computer Output to Laser Disk) device; this is almost certainly now an obsolete technology (The National Archives, 2010, p. 14).

With regard to file formats eight municipalities stated that they experienced access issues. This clearly presents digital continuity risk exposure as information in unsustainable file formats becomes inaccessible over time. This finding can be considered to be relatively high given that national guidance in the form of eTransformation Interoperability Principles was first published in 2005 for all public bodies to follow. The eTransformation Interoperability Principles have been updated and continue to provide guidance on sustainable file formats (Birlikte Çalışabilirlik Esasları Rehberi, 2012, p. 9-12), thus reducing digital continuity risk exposure across the public sector in Turkey. It is ultimately the responsibility of the CIO, or equivalent, in municipalities to ensure that staff have access to, and implement, the guidance in terms of file formats and other issues.

5.4. Policies Relating to Digital Continuity

The seventh to ninth survey questions focused on the existence of policies that ensure that digital continuity risk exposure is minimalised. The three survey questions probed whether municipalities had a digital continuity policy, a policy on data migration and a policy on file formats. Almost half of respondents (48 per cent) stated that their organisation had a digital continuity policy, whereas 33 per cent stated that their organisation did not. Almost 19 per cent of respondents stated that a digital continuity policy was at planning or implementation stage. A similar picture exists regarding the eight question that asked whether municipalities had a policy on data migration in place, with 48 per cent of respondents stating that there was such a policy in place, compared to 37 per cent that stated that a policy on data migration did not exist. With regard to the ninth question, an astounding 74 per cent of respondents answered that their municipality had a policy on file formats. The high rate of municipalities that have a policy on file formats is not surprising considering that, as mentioned above, compulsory eTransformation Interoperability Principles exist that all public bodies have to follow.

Municipalities do not necessarily have to use the same terminology as the current study to denote that a particular practice or policy exists. It is a possibility that respondents interpret the term policy loosely

and may also count strategy documents as policy. The need for archival and information management policies in local government was stressed by *The Final Declaration of the International Symposium on Library and Archive Services of Municipalities* that took place in Turkey in 2016. The symposium also highlighted that information professionals should be employed in archival and information management positions to increase the efficiency of services (Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu Sonuç Bildirgesi, 2016, p. 278-279).

Given that almost half of the municipalities surveyed state that they have a policy on digital continuity indicates that policies exist in these respective municipalities that have content on information managed as risk, regardless of whether the term 'digital continuity' is used or not. The same applies to the existence of a data migration policy. However, despite the fact that the vast majority of Istanbul based municipalities publish a plethora of policies, digital continuity, information management and data migration policies are generally not among those published. Thus, it is difficult to verify the existence of such written policies. A study carried out by Kandur in 2011, bore similar results with half of the respondents stating that a policy for electronic records management existed. However, Kandur concluded that despite the expertise in the management of electronic records held by some public bodies, the lack of sharing expertise and good practice between public bodies was still an issue (Kandur, 2011, p. 7-11).

The exception to the policies that are not published by municipalities are information security policies. Some municipalities also publish information on the use of ERMS and digital archives. Fatih Municipality for example has information on its website under the heading of IT Directorate on the use of various systems including ERMS and its digital corporate archive (Fatih Belediyesi, IT Directorate). However, the information provided does not constitute policy.

In generalised terms, the survey results demonstrate that information risk is recognised and managed within the context of information security, and information management is viewed within the context of the use of ERMS managed by IT directorates. As mentioned previously, none of the municipalities have records management or information management policies published on their websites. Bağcılar Municipality recently published an Integrated Management System policy under which several policies under the heading of Information Security are published. Policies on the use of removable media, change management, e-mails and software procurement appear as headings on the municipality website but are not published. Although the term digital continuity is not used, the policies put in place by Bağcılar Municipality can be said to lower digital continuity risk exposure through having policies for staff to follow on such areas that attract risk such as software procurement or the use of removable media (Bağcılar Belediyesi Entegre Yönetim Sistemi Politikası, 2019). As another example, Beşiktaş Municipality was recognised for the excellent use of its digital assets in 2016, criteria for the award included visibility and management of corporate social media accounts (Dijital Varlıkları En İyi Kullanan İlçe Belediyesi, 2016). However, the long-term preservation of social media content shared by municipalities is an information management issue that is yet to be tackled in Turkey.

5.5. Digital Continuity Training

The tenth survey question probed whether respondents thought that municipalities should run in-house digital continuity training. An overwhelming 96 per cent of respondents stated that municipalities should provide training on digital continuity. The very high rate of respondants who showed a willingness to receive training demonstrates that there is an appetite for training on how to manage information risk amongst information professionals working in municipalities in Istanbul. The UK Scoping Report found that 62 per cent of local authorities provided training on information risk and management, but only half of these said the training was extended to temporary and contract staff (The National Archives, 2010, p. 13). The Scoping Report also noted that training to be too theoretical or high-level, and that there was a lack of practical guidance which can actually be applied by local authority practitioners (The National Archives, 2010, p. 15). The UK National Archives has been offering training and guidance for several years to public bodies on digital continuity, therefore the challenges faced with training may also be encountered in Turkey if training specifically on digital continuity is undertaken.

Training should help municipalities to identify digital continuity risks and to form an action plan. They should be able to describe each risk, including the business consequences of a loss occurring, and ensure

that risks to digital continuity are also captured in other risk registers where appropriate (The National Archives, 2017b, p. 14). For example, saving digital information without specifying how long it will be retained for is a risk, as is using third party suppliers who do not understand compliance.

Table 5

Formulation of Policy on Digital Continuity

Responsibility for formulation of policy	
Information and Communication Technologies Authority (BTK)	6
Turkish State Archives	4
Turkish Standards Institution (TSE)	2
Universities	2
Presidency of Digital Transformation Office	1
Presidency of Strategy and Budget	1
Ministry of Interior	1
Ministry of Environment and Urbanisation	1
Scientific and Technological Research Council of Turkey (TÜBİTAK)	1
In-house	1
Private sector/EDRMS firms	1

The eleventh and final survey question posed to municipalities was as follows: Which organisation do you think should formulate policy on digital continuity in Turkey? The answers to this question are varied as can be seen in Figure 5, and only 19 of the 23 municipalities surveyed answered this question. However, several respondents specified more than one organisation that it believed should formulate policy on digital continuity, and this is reflected in Figure 5. The answers given to this question demonstrate that there is a divergence of opinion amongst information professionals in municipalities on which organisation should be responsible for policy in this area. The most popular answer was the Information and Communication Technologies Authority (BTK) whose remit is to perform regulatory and supervision duties in the electronic communication sector. The mission of the BTK is to shape national policy on information and communication technologies, therefore it isn't surprising that 32 per cent of respondents thought that BTK should formulate policy on digital continuity.

The second most popular answer at 26 per cent was the Turkish State Archives. The archives has a legal remit to receive transfers of records from public sector organisations, including municipalities. Section 11(f) of the 2018 Presidential Decree on state archives, states that the archive is responsible for establishing the method for the transfer of digital records (Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi, 2018). Within the context of the above, the proportion of respondents stating that the State Archives should have responsibility for formulating policy on digital continuity could have been higher, especially given that the archives have the legal remit regarding the transfer of records. Digital continuity refers to using digital information for as long as required for business purposes but, unless the continuity of digital information is managed effectively, it is unlikely to survive to the age at which it should be transferred to the archives. This is why, as is the case in the United Kingdom, that national archives should have the policy lead on digital continuity. The plethora of different organisations cited as those who should lead on digital continuity policy indicates that some ambiguity exists among information professionals in municipalities on this issue. As shown in Figure 5, the answers ranged from the Scientific and Technological Research Council of Turkey (TÜBİTAK), Türksat Satellite Communications and Cable TV Operations Company, to the Ministry of Environment and Urbanisation, and the Turkish Standards Institution. Even though different organisations such as the Turkish Standards Institution have a role in ensuring public bodies manage their digital information to national standards, policy on digital continuity should ideally be formulated by the archives for the reasons discussed above.

6. Conclusion

This study examined the digital continuity risk exposure of municipalities in Istanbul by determining the degree to which digital continuity is practised and embedded. The fact that survey data was provided anonymously allowed for some frankness in the answers provided and allowed for an insight into the awareness of digital continuity. Research showed that the use of information management systems was commonplace across municipalities in Istanbul. One respondent stated that "all public sector bodies should use the same ERMS provided centrally by the state." While other respondents stated that instead of employing records management in a hybrid environment that municipalities should first digitalise their paper records before embarking on ERMS/EDRMS implementation. The UK Scoping Report was instrumental in allowing a comparison of problems faced by local authorities in the United Kingdom versus those faced by local authorities in Istanbul. EDRMS implementation began earlier in the United Kingdom thus allowing for an insight into the dilemmas that the Turkish public sector may face over the next few years. The Scoping Report warns against defining information management solely through the use of information management systems, and found it worrying that information management improvements were defined through a single technology or environment (The National Archives, 2010, p. 14). This is a warning that municipalities should also heed, as technology is only one component of digital continuity.

Almost all respondents were unanimous in stating that in-house training on digital continuity should be provided. Indeed, one respondent said that audits should be carried out identifying digital continuity risk in municipalities. There was a divergence of opinon about who should be responsible for providing training, with only some respondents taking the view that the State Archives should provide training. Ideally, it is the Turkish State Archives that should provide digital continuity training given its legal remit to accept digital transfers. In the way of a snapshot into digital continuity practices, it is clear that electronic records management is embedded across municipalities, but this does not translate into managing information within the framework of risk management. Although almost half of the municipalities surveyed state that they have a policy on digital continuity, none of the municipalities surveyed have published policy on digital continuity, other than the guidance published by other public bodies on such topics as file formats.

According to the survey data, almost 45 per cent of municipalities have a Chief Information Officer which is a positive development. However, municipalities did not have defined roles in relation to digital continuity, and IT Directorates were cited most commonly as being responsible for information management. Information professionals, including records manager, do not seem to enjoy a high profile in municipalities. Digital continuity exposure risk remains because the policies and responsibilties side of digital continuity is lacking across municipalities. The emphasis is more on the use of technology rather than the governance surrounding it. Overall, digital continuity practices are not embedded within their own right, but more within the context of EDRMS usage. However, an awareness of digital continuity, and the appetite for training and national guidance is evident.

Compliance with Ethical Standards

Conflict of Interest: The authors declare that there is no conflict of interest.

Ethics Committee Permission: Marmara University Social Sciences Ethics Committee has unanimously decided that this research is ethically appropriate at its meeting dated 05.01.2022 and numbered 2021-139.

Authors Contribution Rate Statement: The authors declare that they have contributed equally to the article.

Financial Support: No

References

5216 Sayılı Büyükşehir Belediyesi Kanunu. *R.G.,* S 25531, 10 Temmuz 2004.

5393 Sayılı Büyükşehir Belediyesi Kanunu. *R.G.,* S 25874, 13 Temmuz 2005.

Adam, A. (2008). *Implementing Electronic Document and Record Management Systems*. Auerbach Publications.

Akdoğan, Z. and Özdemirci, F. (2016, 12-14 Mayıs). Belediyelerde E-Arşiv Uygulamaları ile Dijitalleştirme Çalışmalarında İzlenmesi Gereken Yol Haritası, in Bülent Yılmaz, Tolga Çakmak, Şahika Eroğlu (Eds.), *Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu*, (pp. 208-212). Nilüfer Belediyesi.

Bağcılar Belediyesi (2019). *Entegre Yönetim Sistemi Politikası.* http://bagcilar.bel.tr/kalitepolitikasi

Beşiktaş Belediyesi (2016). *Dijital Varlıkları En İyi Kullanan İlçe Belediyesi.* https://www.besiktas.bel.tr/Sayfa/12037/dijital-varliklari-en-iyi-kullanan-ilce-belediyesi

BKAHS Düzenleme Kurulu (2016). Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu Sonuç Bildirgesi, in *Türk Kütüphaneciliği* 30, 2 (2016), 277-281.

Coventry City Council (2021). *What is Information Governance?* https://www.coventry.gov.uk/info/11/strategies_plans_and_policies/466/data_protection/2#:~:text=Information%20Governance%20can%20mean%20different%20things%20to%20different%20people.&text=It%20allows%20both%20the%20Council,deliver%20the%20best%20possible%20services

Çiçek, N. (2008). Belediyelerde Standart Dosya Planı Uygulamalarında Yaşanan Güçlükler. *Bilgi Dünyası*, 9 (2), 133-153. https://doi.org/10.15612/BD.2008.314

Çiçek, N. (2020). E-Devlet Stratejisi Bağlamında Elektronik Belge Yönetimi İçin "Yazılı Politika" Gereksinimi: Türkiye'deki Uygulamalar Üzerine Bir İnceleme. *Türk Kütüphaneciliği*, 34 (3), 377-405. https://doi.org/10.24146/tk.739591

Devlet Arşiv Hizmetleri Hakkında Yönetmelik. *R.G.,* S 30922, tar. 18 Ekim 2019. www.devletarsivleri.gov.tr/varliklar/dosyalar/mevzuat/arsivhizmetleri.pdf

Devlet Arşivleri Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi. *R.G.,* S 30480, tar. 18 Temmuz 2018. www.devletarsivleri.gov.tr/varliklar/dosyalar/mevzuat/19.5.11.pdf

Digital Preservation Coalition. Digital Preservation Handbook Glossary (2021). https://www.dpconline.org/handbook/glossary#:~:text=Digital%20Preservation%20Refers%20to%20the,for%20as%20long%20as%20necessary.&text=Medium%2Dterm%20preservation%20%2D%20Continued%20access,of%20time%20but%20not%20indefinitely

Erdoğan, O. (2019). Yerel Yönetimlerde E-Belediye Uygulamaları: İçişleri Bakanlığı E-Belediye Bilgi Sistemi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 23 (3), 551-566 https://dergipark.org.tr/tr/download/article-file/1008627

e-Yazışma Projesi ile İlgili 2017/21 Sayılı Başbakanlık Genelgesi. *R.G.,* S 30210, tar. 14 Ekim 2017. https://www.resmigazete.gov.tr/eskiler/2017/10/20171014-11.pdf

Fatih Belediyesi (2020). Stratejik Planı, 2020-24 dönemi. https://www.fatih.bel.tr/images/File/9668a4b9482341d896fb55f5223ec10e.pdf

Fatih Belediyesi (2021). Bilgi İşlem Müdürlüğü web sayfası. https://www.fatih.bel.tr/bilgi-islem-mudurlugu

İcimsoy, O. (2000). Belediyelerde İmar Dosyalarının Belge Profili ve Arşivlerinin Oluşumu: Kartal Belediyesi Örneği. *Arşiv Araştırmaları Dergisi*, (2), 47-62.

Kandur, H. (2011). Türkiye'de Kamu Kurumlarında Elektronik Belge Yönetimi: Mevcut Durum Analizi ve Farkındalığın Artırılması Çalışmaları. *Bilgi Dünyası*, 12 (1), 2-12. https://doi.org/10.15612/BD.2011.218

Kandur, H. (2016). The Role Of İnstitutional Competencies for The Long Term Preservation of Electronic Records: The Experience of the Turkish Public Sector. *Qualitative and Quantitative Methods in Libraries (QQML)* 5: 527-533.

Moss M., Thomas D. and Gollins T. (2018). Artificial Fibers: The Implications of the Digital For Archival Access. *Frontiers in Digital Humanites*. 5:20. https://doi.org/10.3389/fdigh.2018.00020

National Archives of Australia (2021). Information Governance. https://www.naa.gov.au/information-management/information-governance

Nottinghamshire County Council (2018). Information Governance Framework. https://www.nottinghamshire.gov.uk/media/132580/information-governance-framework-v10.pdf

Özdemirci, F. (2016, 12-14 Mayıs). Belediyelerde Elektronik Belge Yönetim Sistemlerinin Boyutu ve Kurumsal Yapılanma Gereksinimleri. *Belediyelerin Kütüphane ve Arşiv Hizmetleri Uluslararası Sempozyumu*, (Powerpoint presentation).

Pearce-Moses, R. (2005). *A Glossary of Archival and Records Terminology*. Society of American Archivists.

Pektaş, E. K. (2011). Belediye Hizmetlerinde Bilgi-İletişim Teknolojilerinin Kullanımı ve E-Belediye Uygulamalarındaki Son Gelişmeler: Bir Literatür Taraması. *Afyonkarahisar Üniversitesi Sosyal Bilimler Dergisi*, 13 (1), 65-88.

Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik. *R.G.,* S 31151, tar. 14 Ekim 2020.https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2646&MevzuatTur=21&MevzuatTertip=5

T.C. Kalkınma Bakanlığı (2012). *e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi (Sürüm 2.1)*. Bilgi Toplumu Dairesi Başkanlığı. http://www.bilgitoplumu.gov.tr/wp-content/uploads/2014/04/Birlikte_Calisabilirlik_Esaslari_Rehberi_2.1.pdf

The National Archives (2010). Scoping Report to The National Archives on the Local Government Digital Continuity Requirement. https://www.nationalarchives.gov.uk/documents/information-management/report-to-tna-on-local-authority-digital-continuity-v1-0.pdf

The National Archives (2017a). Information Asset Factsheet. https://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

The National Archives (2017b). Risk Assessment Handbook. https://www.nationalarchives.gov.uk/documents/information-management/Risk-Assessment-Handbook.pdf

The National Archives. What is Digital Continuity? (N.d.) https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/what-is-digital-continuity

Türk Standartları Enstitüsü 13298. (2015). Elektronik belge ve arşiv yönetim sistemi standardı.

Union of Municipalities of Turkey (2021). Municipalities in Turkey. https://www.tbb.gov.tr/en/local-authorities/municipalities-in-turkey