Jurnal Teknik Indonesia (Ju-Ti)
Vol. 5, No. 02, 2026, pp. 278-284
https://jurnal.seaninstitute.or.id/index.php/juti

Improving Data Security through Data Security Implementation in the Public Sector Based on DMBOK

Firmansyah[1], Agus Yulianto[2], Budi Sudrajat[3], Mulia Rahmayu[4], Asri Wahyuni[5]
Faculty of Information Technology, Bina Sarana Informatika University, Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Kec. Senen, Kota Jakarta Pusat, Indonesia
Email: firmansyah.fmh@bsi.ac.id

Public sector institutions manage large volumes of data, ranging from public information to sensitive records, yet data breaches continue to disrupt public services and erode public trust. Many institutions lack a structured way to translate data protection regulations into operational security policies. This study proposes a stepwise approach to implementing data security in public sector institutions based on the DAMA-DMBOK data security knowledge area, supported by the COBIT 2019 framework. The approach has five stages: identifying business and regulatory requirements, developing standards and policies, implementation, evaluation, and improvement. Requirements are analyzed using the confidentiality, integrity, and availability (CIA triad) and a data criticality classification, with health data as an illustrative case. The standards and policies are then mapped to COBIT 2019 processes in the EDM, APO, BAI, DSS, and MEA domains. The mapping yields twelve COBIT processes, each linked to specific policy documents, such as information security, access control, data protection, incident response, and business continuity policies. Each policy is further broken down into standard operating procedures, standards, technical guidelines, and forms. The approach gives public sector institutions a structured way to identify critical data assets and establish accountable information security governance. It remains a conceptual proposal that has not been validated empirically, so future work should test it through case studies in government agencies.
Keywords: CIA triad; COBIT 2019; DMBOK; information security governance; public sector; security policy

This is an open access article under theCC BY-NClicense

Corresponding Author:
Agus Yulianto
Faculty of Information Technology, Bina Sarana Informatika University
Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Kec. Senen, Kota Jakarta Pusat
agus.aag@bsi.ac.id

1. Introduction

The public sector generally consists of government agencies or bodies whose assets and management are supervised by the government, such as ministries, state agencies, local governments, law enforcement agencies, and other government bodies. This sector is important because many of its institutions serve the public directly and store millions of transactions in large databases. The large volume of data they manage includes population, health, taxation, financial, and education records, as well as other strategic information of high value to government institutions. Therefore, data security is a crucial aspect of ensuring the continuity of public services and maintaining public trust in the government [1]. Data security in the public sector focuses not only on protecting confidentiality but also on ensuring data integrity and availability. To achieve these goals, public sector organizations need effective information security governance, continuous risk management, adequate access control, security awareness programs for employees, and appropriate information security standards and frameworks. In this way, public data can be protected from various threats, and government services can run securely, reliably, and sustainably [2].

ISSN 2964-0490

2. Literature Review and Problem Statement

Previous Research

The many data security incidents that currently affect companies have made data security an important issue, and companies must invest in it to keep their data safe. Data breaches are caused by both technical and non-technical factors. Technical problems, such as ransomware attacks and malicious software that lead to data theft, are among the most common attacks today. Non-technical problems generally include the absence of a policy to adopt standards such as DMBOK (Data Management Body of Knowledge), COBIT, or ISO 27001, which increases data security risk. One widely used standard for implementing data security is DMBOK, which defines 10 domains, one of which is data security.

Many studies have been conducted on data security, including studies of data security in public services, particularly the recent data leak at the Ministry of Communication and Information Technology (Kominfo). That study identified six weaknesses that caused the leak: a lack of technical skills, human error, a shortage of data security personnel, low accountability, insufficient data security regulation, and infrastructure problems [3]. Data security issues also include attacks such as ransomware and phishing, as well as data leaks and human error [4]. Beyond public sector data security, data security in cloud computing and big data has also been a research focus [5] and [6] reported several data security issues, such as data leaks, malicious software, and a lack of data security personnel. In the health sector, [7] stated that medical records are personal data that must be protected and that data security covers three aspects: confidentiality, integrity, and availability.

Personal Data Protection

In the context of cyber law and digital data governance, "PDP" stands for *Pelindungan Data Pribadi* (Personal Data Protection). In Indonesia, this framework has been strengthened through Law Number 27 of 2022 concerning Personal Data Protection (the PDP Law), which serves as an overarching digital regulation designed to safeguard citizens' sensitive data against threats such as leaks, misuse, or illegal sale. The PDP Law establishes data as the object of protection and imposes strict legal obligations on data controllers. Consequently, data controllers are legally responsible for ensuring the security of such data, including in the event of a protection failure or a data breach. [8]

Data Security

Data is a collection of information that includes symbols, words, numbers, sounds, images, video, and other sources of information. Data and information are inseparable: data is the embodiment of information, while information is the meaning contained in data. Data sometimes contains personal details, so an organization needs to protect its data for specific purposes; this practice is known as data security. Data security comprises a set of standards, technologies, frameworks, and related processes that focus on protecting data from unauthorized access and from damage throughout its lifecycle [9]. In some cases, data contains the personal information of the data owner, and the owner does not permit it to be shared with unauthorized entities. Several issues weaken data security, particularly in the public sector, such as the government's not yet optimal role in enforcing data security policies and a lack of multisector cooperation between the government and the private sector in implementing data security [10]. Vulnerable data security in the public sector disrupts public services and ultimately erodes public trust in the government [11] .

COBIT 2019

In implementing data security in the public sector, one framework that can be combined with DMBOK is COBIT 2019. COBIT 2019 is an IT governance framework developed by ISACA (Information Systems Audit

ISSN 2964-0490

and Control Association). Applying COBIT 2019 can strengthen an organization's internal IT policies and align organizational goals with sustainable operations [12] . COBIT 2019 has five domains: EDM (Evaluate, Direct, and Monitor), APO (Align, Plan, and Organize), BAI (Build, Acquire, and Implement), DSS (Deliver, Service, and Support), and MEA (Monitor, Evaluate, and Assess) [13]. COBIT 2019 benefits IT governance by supporting the alignment of IT strategy with the organization's vision, mission, and goals, providing assurance of IT services, and managing risk to protect public institutions from disruption and threats [14].

3. Method

Implementing a data security standard requires several steps, starting with determining data security requirements, then defining data security policies, implementing them, and evaluating the policies. The following diagram shows the data security implementation process:

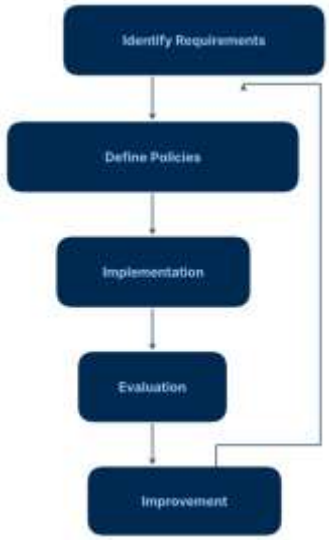


Figure 1 Steps Of Data Security Implementation

Requirements identification

Data security requirements come from two sources: business (internal) requirements and regulatory (external) requirements. Business-driven data security is the standard that an institution wants to achieve to meet its own needs, and it generally differs from one institution to another. To determine these requirements, they need to be discussed with the stakeholders within the institution. For requirements that come from government regulation, the government generally issues policies, regulations, or laws governing data security. Policies created within public sector institutions must refer to the existing regulations and laws [15]. To analyze these requirements, TOGAF-ADM can be used to identify the data that must be protected and to classify the data using the Confidentiality, Integrity, and Availability (CIA) concept. In the health sector, data identification takes the following form:

Table 1 Data criticality identification

Data	Criticality Level
Data name	Very high/High/Medium/Low/Very low
.....	.....

After identifying the data and its criticality level, enter them into the CIA matrix below:

ISSN 2964-0490

Table 2 CIA matrix

Data	Confidentiality	Integrity	Availability
Patient	Very high	Very high	Very high
.....			

Developing standards and policies

The standards that can be used to implement data security requirements are ISO 27001 or COBIT. COBIT can be implemented by first conducting an assessment. For the EDM (Evaluate, Direct, and Monitor) domain, EDM03 (Ensure Risk Optimization) can be used, while for the APO domain, APO01 (Managed IT Management Framework), APO12 (Managed Risk), and APO13 (Managed Security) can be used. The details are as follows:

Domain	Domain Detail
EDM (Evaluate, Direct, Monitor)	EDM03 (Ensure Risk Optimization)
APO (Align, Plan, Organize)	APO01 (Managed IT Management Framework)
	APO12 (Managed Risk)
	APO13 (Managed Security)
BAI (Build, Acquire, and Implement)	BAI03 (Managed Solutions Identification and Build)
	BAI06 (Managed IT Changes)
DSS (Deliver, Service, and Support)	DSS01 (Managed Operations)
	DSS04 (Managed Continuity)
	DSS05 (Managed Security Services)
	DSS06 (Managed Business Process Control)
MEA (Monitor, Evaluate, and Assess)	MEA02 (Managed System of Internal Control)
	MEA03 (Managed Compliance)

Implementation

This stage continues from the implementation of the standards and policies established earlier. With the involvement of the stakeholders concerned, particularly the information technology division from the IT director down to staff level, all documents related to the standards and policies begin to be carried out. To improve compliance with the standardized processes, internal and external audits are needed to ensure that all standards and policies are properly executed.

Evaluation

Auditing procedures, standards, or policies is one part of the evaluation process, which aims to test the compliance and suitability of the policies that have been created. Beyond auditing, the institution needs to evaluate its policies periodically to assess whether they remain relevant to internal needs and consistent with current laws and regulations. If a policy is no longer relevant, it must be revised, adjusted, or removed from the existing policies. IT audits may involve third parties or vendors to ensure that the policies conform to the standards.

Improvement of standards and policies

After all procedures and policies have been documented and implemented in the institution, some policies may need to be corrected or enhanced during the process so that IT governance in the institution improves.

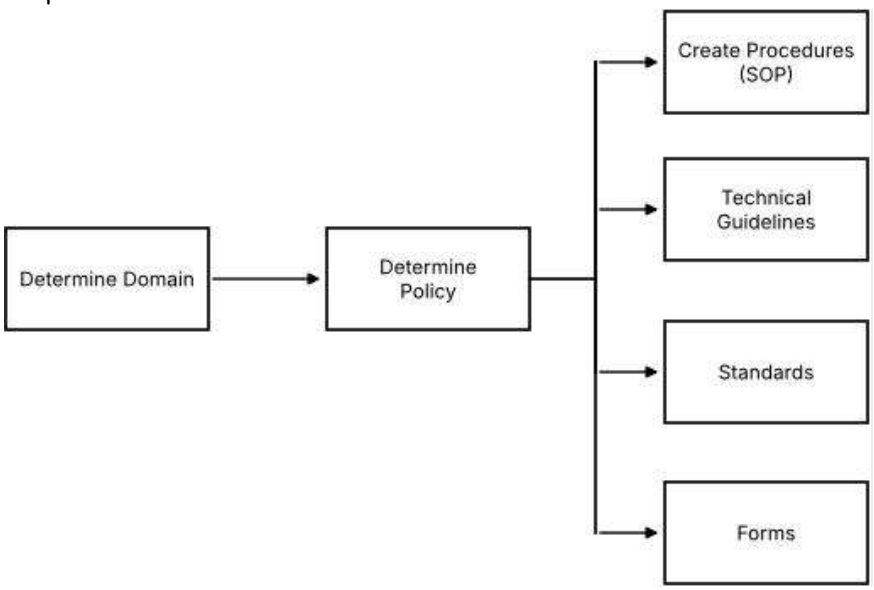
4. Results And Discussion

To implement data security using COBIT, the institution needs several policies, as follows:

ISSN 2964-0490

Domain	Policy Document
EDM03	Information Security Risk Management Policy
APO01	IT Governance and Information Security Policy
APO12	Risk Identification, Analysis, and Mitigation Policy
	Vulnerability Policy
APO13	Information Security Policy
	Access Control Policy
	Data Protection Policy
BAI03	Secure System Development Life Cycle Policy
BAI06	Change Management Policy
DSS01	IT Operations and Infrastructure Management Policy
DSS04	Business Continuity and Disaster Recovery Policy
DSS05	Security Operations and Incident Response Policy
	Logging and Monitoring Policy
DSS06	Access Control and Segregation of Duties Policy
	Data Retention and Disposal Policy
MEA02	Internal Audit and IT Internal Control Policy
MEA03	Regulatory and Standards Compliance Policy

Each policy in each domain is broken down into Standard Operating Procedures (SOPs), standards, technical guidelines, and forms. For example, an access control policy can be broken down into procedures for requesting access rights, deactivating users, and managing access rights, along with other related procedures. The overall process can be illustrated as follows:



5. Conclusion

This study presented a five-stage approach to implementing data security in public sector institutions based on DMBOK and supported by COBIT 2019. Requirements are identified from business and regulatory needs and classified using the CIA triad. Standards and policies are then mapped to twelve COBIT 2019 processes across the EDM, APO, BAI, DSS, and MEA domains, and each policy is translated into standard operating procedures, standards, technical guidelines, and forms. Implementation, periodic evaluation including internal and external audits, and continuous improvement keep the policies relevant and compliant with

current regulations. The approach helps institutions identify critical data assets and build accountable security governance. Because it has not yet been validated empirically, future research should apply it in government agencies, for example in the health sector, and measure its effect on regulatory compliance and security maturity.

6. Referensi

[1] L. Magnusson, S. Iqbal, P. Elm, and F. Dalipi, "Information security governance in the public sector: investigations, approaches, measures, and trends," *Int. J. Inf. Secur.*, vol. 24, no. 4, Aug. 2025, doi: 10.1007/s10207-025-01097-x.

[2] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Understanding Local Government Cybersecurity Policy: A Concept Map and Framework," *Information (Switzerland)*, vol. 15, no. 6, Jun. 2024, doi: 10.3390/info15060342.

[3] R. Rambe and F. F. Hermawan, "The Impact of Ransomware on Indonesia's National Data Security: Case Study of Kominfo Data Leaks," *Indonesian Journal on Computing (Indo-JC)*, vol. 10, no. 1, Aug. 2025, doi: 10.21108/indojc.v10i1.8976.

[4] A. K. Putri, A. Nurmandi, M. Younus, H. Lawelai, W. Suardi, and A. Zainudin, "Comprehensive Analysis of Data Security Threats in the Public Sector," *Journal of Governance*, vol. 10, no. 3, Sep. 2025, doi: 10.62870/jog.v10i3.29903.

[5] S. Azhar *et al.*, "Big Data Security Issues: A Review," 2023.

[6] S. M. Reddy, M. Sana, M. Sushma, M. Divya Sri, and U. G. Student, "Enhanced Data Privacy and Security in Cloud Storage: A Robust Authentication Scheme for Cyber-Physical-Social Systems," *Journal for Educators, Teachers and Trainers JETT*, vol. 15, no. 5, pp. 383–392, 2024, doi: 10.47750/jett.2024.15.05.38.

[7] Adi Ahmad, Yusmanidar, J. Hastuti, M. Hijriatin, and Sarno, "Data Security Analysis in Electronic Health Information Systems," *Journal Informatic, Education and Management (JIEM)*, vol. 7, no. 1, pp. 1–11, Feb. 2025, doi: 10.61992/jiem.v7i1.107.

[8] N. Alfiana Alfitri, "Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Journal Social Society*, vol. 4, no. 2, p. 2024, doi: 10.30605/jss.4.2.2024.511.

[9] A. Wang, "An Introduction to Data Security," 2025. doi: https://doi.org/10.1142/9789819800285_0001.

[10] J. Catherine *et al.*, "DAMPAK KEBOCORAN DATA PRIBADI TERHADAP PENINGKATAN CYBER SECURITY AWARENESS DI INDONESIA: A SYSTEMATIC LITERATURE REVIEW," *Jurnal IMAGINE + JURNAL IMAGINE*, vol. 5, no. 2, [Online]. Available: https://jurnal.idbbali.ac.id/index.php/imagine

[11] A. Sarjito, "Data Security and Privacy in the Digital Era: Challenges for Modern Government," *Jurnal Ilmiah Administrasi Negara)*, vol. 8, no. 2, pp. 1–13, 2024.

[12] D. Putra, A. Putera, and U. Siahaan, "COBIT 2019 for IT Governance Evaluation: A Cross-Sector Systematic Review," *Journal of Technology and Computer (JOTECHCOM)*, vol. 3, no. 2, pp. 94–102, 2026.

[13] Munaspin Zahra Diva Putri, Indah Dwi Rosa, and Baturohmah Habi, "12 View of IT Governance Maturity Assessment of the BRAVO Application Using an Integrated COBIT 2019 and ITIL 4 Framework," *JUSIFO (jurnal sistem informasi), Vol. 11, No. 2 (2025)*, 2025, doi: https://doi.org/10.19109/jusifo.vlli2.31602.

[14] M. D. S. Antariksa, M. P. Angin, and A. P. Widodo, "COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry

ISSN 2964-0490

Sectors," *Journal of Renewable Energy, Electrical, and Computer Engineering*, vol. 5, no. 1, pp. 99–105, Mar. 2025, doi: 10.29103/jreece.v5i1.19501.

[15] N. Setio Wibowo, E. Utami, and H. Al Fatta, "Perancangan Struktur Tata Kelola Data di Pemerintah Daerah Menggunakan Framework Data Management Body Of Knowledge Designing Local Government Data Governance Structure Using the Data Management Body Framework of Knowledge," *Research : Journal of Computer*, vol. 4, no. 1, pp. 45–52, 2021.