Journal of Namibian Studies, 36 S2 (2023): 539-551 ISSN: 2197-5523 (online)

The Contribution Of It Audit To Data Governance

Hamza Rabii[1], Hicham Drissi[2], Ayoub Gacim[3]

[1] LIFGOD ENCG CASABALNCA
hamzarabii@hotmail.com

[2] LIFGOD ENCG CASABALNCA
h.drissi@encgcasa.ma

[3] LIFGOD ENCG CASABALNCA
gacim.ayoub@gmail.com

Abstract

This paper reviews the existing literature addressing related issues Knowledge on information systems audit and Data governance. this review is important owing to the increase of technology in the recent year, The Information technology has become the core of the company's business. This technological progress that materializes in the digitalization of data and their volumetrics is a significant step in the world of management but also a handicap for classic audit. Our review covers three wide parts. First, we explore the environment of information system Audit. Second, we present the Data governance. Third, the contribution of IT audit to data governance for Moroccan SMEs.

Keywords: AUDIT, Information System, COBIT, Data Governance.

Introduction

There are different types of data. For example, with the emergence of social media, data about customers' online behavior can be generated, such as clickstream records taken by users on a corporate website, call details and data usage records of telecommunications companies, as well as data files, Transaction. The equipment continuously produces streams of data and events. Transactions data from medical images and health data continue to be generated in mission-critical traditional applications.

In 2006 there was a survey. It was reported that a data governance program was one of five successful practices that extract business value from data assets.[1] . Over the past century, some organizations still lacked knowledge of the data they possessed, its criticality, the critical data sources that exist, or the degree of redundancy of their data assets. Data governance is an important topic for any organization that recognizes the importance of its business data as the foundation of its success in recent years. Business management looks at decision-making and data authority.

Review Literature

a) Audit for Information systems

An information system is more than just a computer. Today's information systems are complex and there are many components that combine to model a business solution. ensure Information about an information system can only be obtained if all components are evaluated and protected. The principal elements of IS audit can be divided as follows [2]:

a) Physical and environmental review: this part contains physical security, Environmental factors such as power supply, air conditioning, humidity control, etc.

b) System Administration review: This includes a security review of operations systems, database management systems, all system management procedure.

c) Application software review: The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business the review of the application software is checking access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures

d) Network security review: Typical coverage areas include internal and external connections to the system, perimeter security, firewall examination, router access control lists, port analysis, and intrusion detection.

e) Business continuity review: This includes the existence and maintenance of redundant and fault-tolerant equipment, backup, and storage procedures, as well as documented and tested disaster recovery and business continuity plans.

f) Data integrity review: the objective is to review the data in real time to verify the adequacy of controls and the impact of weaknesses, as indicated in the above reviews.

Every Organizations uses various information systems, the auditor should answer three basic question what to audit, when and how frequently.to archive it’s a goal is to adopt a risk-based approach.

Organizations face daily the inherent risk of information system. These risks affect uncommon systems in different ways. The risks of nonviability of information systems even for little moment can make the organizations lose a big profit, the risk of unauthorized access can be the sources of a potential fraud, the technical environment in which the system operates also affects the risks associated with the system.

1. COBIT

COBIT (Control Objectives for Information and Related Technologies) is framework elaborate by ISCA (information Systems Audit and Control Association). It's the most popular framework of controlling information system, it's appearing the first time in 1996, the last version 5 Cobit was published in 2012.

COBIT 5 includes a set of guidelines and best practices for governance and management across all areas of IT (such as security, risks, etc.)

The principles and enablers of COBIT 5 are generic and applicable to all companies whatever the size, whether commercial, not-for-profit, or public sector.

Fig. 1. COBIT 5 principles [3]

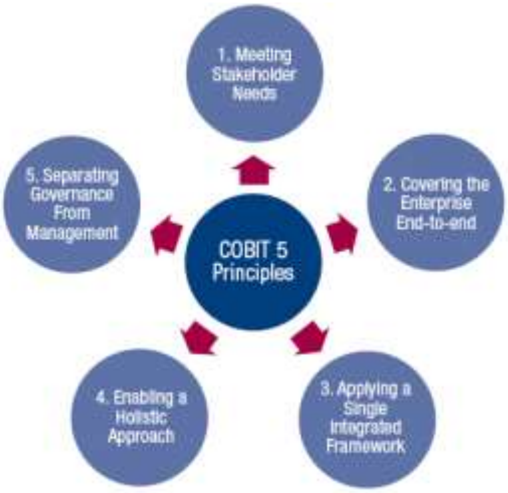
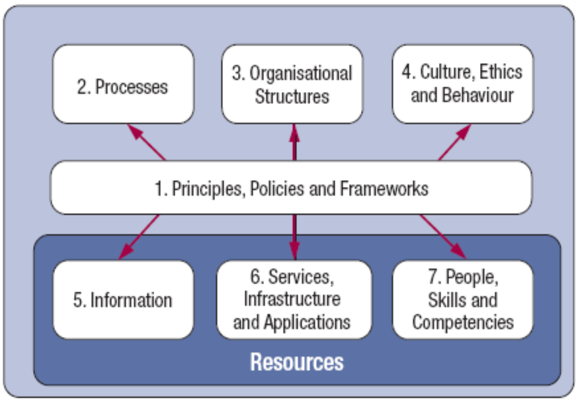

1. Meeting Stakeholder Needs
5. Separating Governance From Management
COBIT 5 Principles
2. Covering the Enterprise End-to-end
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

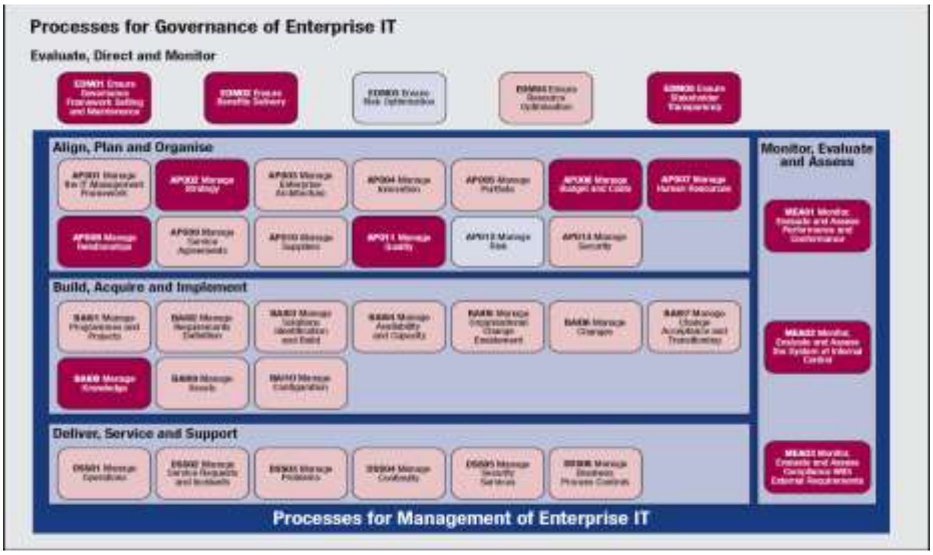
Fig. 2. COBIT 5 enablers [3]


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

COBIT5 contains 34 control objectives and 37 processes, the completion of which can successfully achieve the goals of a functional information system. which are grouped into five domains, in turn are divided into two large areas [4],[5]:

- Governance: established by one domain (Evaluate, Direct and Monitor (EDM)), which include five process.
- Management: incorporate four domains, which represent the areas of Plan, Build, Run and Monitor (PBRM):
    - Align, Plan and Organise (APO): 13 processes
    - Build, Acquire and Implement (BAI): 10 processes
    - Deliver, Service and Support (DSS): 6 processes
    - Monitor, Evaluate and Assess (MEA): 3 processes

Fig. 3. COBIT 5 processes [3]


Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor
Align, Plan and Organise
Monitor, Evaluate and Assess
Build, Acquire and Implement
Deliver, Service and Support
Processes for Management of Enterprise IT

b) Data governance

Data governance is a broad concept that encompasses the management of data assets within an organization. It involves various aspects such as availability, integrity, security, decision-making rights, responsibilities, policies, processes, and technologies. While different researchers may have slightly different perspectives on data governance, there are some common themes.[6]

Some researchers argue that data governance and information governance are distinct concepts. They highlight that data governance primarily focuses on managing data assets, ensuring their quality, security, and availability. On the other hand, information governance is concerned with the interactions and usage of information within an organization, including processes, systems, and compliance with regulations.

Thomas [7] presents data governance as a system of decision rights and responsibilities. It involves establishing agreed-upon models that define who can take specific actions with certain information, under what circumstances, and with what methods. Data governance is considered crucial for making authoritative decisions and ensuring desirable behavior in the use of data.

To promote desirable behavior, data governance develops and implements enterprise-wide policies, guidelines, and data standards consistent with the organization's goals, strategy, values, and culture. This helps establish a framework for decision-making rights and responsibilities and encourages responsible data use.[6]

In addition to decision-making, data governance also encompasses policies, processes, technologies, and responsibilities related to data control and management. It includes defining the purpose of data collection, governing data ownership, and specifying permissible use of data. Rosenbaum suggests that data governance involves establishing general policies for accessing, managing, and using data in a manner that aligns with the organization's objectives.[6]

Overall, data governance involves a comprehensive approach to managing and controlling data assets, ensuring their quality, security, and appropriate use throughout their lifecycle within an organization.

Researchers emphasize the significance of data governance in managing data assets within an organization. Data governance is seen as a way for organizations to effectively handle their digital data and recognize its strategic value.[8] It encompasses a convergence of various elements such as procedures, technologies, processes, policies, responsibilities, and decision-making rights related to data usage.

The accountability for decision-making regarding data assets lies with the individuals or entities holding decision-making rights. In a data governance framework, there are five interconnected decision areas that guide the organization's approach to data management. These decision areas are illustrated in Figure 4 (not provided), which likely represents a visual representation of the framework. At the top of the framework are the data principles that establish the overarching guidelines and requirements for data usage within the organization.[1]

The data principles define the intended uses of the data, which in turn establish the organization's data quality standards. These standards serve as the foundation for interpreting and accessing the data by users. Furthermore, data lifecycle decisions, which involve managing data throughout its lifecycle, play a crucial role in operationalizing the data principles within the organization's IT infrastructure.

Overall, the proper implementation of data governance enables organizations to effectively manage their data assets, make informed decisions, ensure data quality, and align data usage with organizational objectives and requirements.

Fig 4: Decision domains for data governance [1]

<table>
<tr><td colspan="3">MAIN DATA</td></tr>
<tr><td rowspan="2">Data Quality</td><td>Meta Data</td><td rowspan="2">Data life cycle</td></tr>
<tr><td>Data Access</td></tr>
</table>

Principles of data [1]:

The principles of effective data establish a connection between data governance and the organization's activities. By standardizing business processes, there is an implicit recognition of a clearly defined owner of data assets. These data principles determine the extent to which data is considered an enterprise-wide asset and dictate the appropriate policies, standards, and guidelines.

Data principles also promote opportunities for data sharing and reuse, aligning with the concept of data as an asset. Each principle is accompanied by a set of implications that further clarify its application. Additionally, the data principles take into account external data sources, such as customer data obtained from third-party service providers. The regulatory environment surrounding data usage is also considered when formulating an organization's data principles.

The data principles serve to define desirable behaviors for both information systems professionals and business users. Business users, acting as data owners, have a significant role in managing data quality, lifecycle management, interpretation, and access. Information systems professionals, on the other hand, fulfill the role of data stewards, utilizing IT tools to assist data owners in identifying and addressing data quality issues.

Overall, the data principles form a crucial component of data governance, guiding the behaviors and responsibilities of both business users and information systems professionals in managing data effectively.

Data Quality [1]:

Poor data quality can have significant operational and strategic implications for a business. Similar to product quality, data quality is a vital aspect that organizations need to consider. Data quality encompasses dimensions such as accuracy, timeliness, completeness, and credibility. However, these dimensions are relative and must be defined in the specific context of how the data will be used.

For instance, an insurance company targeting physicians as potential customers may find 85% accuracy acceptable for physician name, address, and phone number. However, organizations that need to notify physicians of a drug recall would require a higher level of accuracy. The acceptability of data quality is determined based on its alignment with the intended use of the data.

Ensuring data accuracy involves matching the recorded values with the actual values in relation to the intended use. Timeliness refers to the data being up to date and reflecting the current state of affairs. Completeness relates to recording all the necessary values and ensuring an adequate depth of information. Credibility focuses on the reliability of the data source and the content it provides.

The data quality decision-making area within data governance involves roles such as data quality officers, data quality analysts, data quality trainers, and subject matter experts. These roles establish standards for different dimensions of data quality, develop mechanisms for ongoing communication of the commercial uses of data, and make critical decisions regarding data quality. Effective data quality decisions are crucial for the successful governance of data assets within an organization.

Meta Data [1]:

Metadata plays a crucial role in describing the content and meaning of data, enabling its interpretation and facilitating data management within an organization. There are various types of metadata, including physical, domain-independent, domain-specific, and user metadata.

Physical metadata provides information about the physical storage of data at the lowest level, such as the location and format of the data. It includes details about data creators, modifiers, authorization, audit trails, and lineage information. This type of metadata establishes a link between the database and the real world by mapping representation languages to agreed-upon real-world concepts.

At the organizational level, metadata describes application data for individual units, supporting specific descriptions of data within those units. At the divisional level, metadata aids in reconciling domain-specific descriptions across the entire organization. Users can also associate annotations with data items or collections, capturing preferences and usage history.

The intended use of data and its lifecycle management influence its utilization within an enterprise. Roles such as enterprise data architects and data modeling engineers are responsible for making decisions related to metadata, particularly in the domain of data retrieval and analysis. Standardizing metadata ensures effective utilization and tracking of information, enabling data to be properly interpreted.

As the business environment evolves, organizations need to adapt their practices accordingly. Metadata allows for monitoring and keeping track of changes, ensuring that data remains relevant and aligned with evolving business needs and requirements.

Access Data [1]:

The ability of data recipients to assign value to different categories of data determines their access privileges. Data security officers play a crucial role in conducting effective risk analysis to identify the data needs of the organization and establish safeguards to ensure confidentiality, integrity, and availability of data. Risk assessment is integrated into an organization's legal and regulatory compliance efforts, with industry standards serving as a guide for formulating and updating access policies and standards.

Data access standards are based on defining "unacceptable" uses of data, as well as implementing mechanisms to track data access and modifications, ensuring confidentiality and availability. Data access decisions provide standards at both the physical and logical levels. Physical data integrity standards protect data from physical damage, while logical data integrity standards preserve the structure of databases.

By developing enterprise-wide and integrated data access decisions, organizations can streamline data migration processes and facilitate automation. This allows for efficient and secure data transfer within the organization.

Overall, data access decisions and standards play a vital role in managing data security, ensuring appropriate access privileges, and maintaining data integrity throughout its lifecycle.

Data lifecycle [1]:

The design of data governance relies on understanding the lifecycle stages that data goes through. The value of data can change as it moves through different stages, such as in the case of a patient's diagnostic information in an electronic medical record during surgery and transfer to an intensive care facility. By comprehending data usage patterns and retention requirements, organizations can develop strategies to align storage media with optimal usage.

However, many organizations face challenges in understanding their data inventory, the importance of data, available data sources, and data redundancy. Information chain managers play a crucial role in managing the inventory of data and its diverse sources. They develop an understanding of common and least common types of data, storage needs, and growth trends. Service level agreements for data access and use can also be integrated as metadata, and a data taxonomy can assist in data lifecycle management.

Efficient data distribution across multiple resources can be achieved by placing data on the appropriate storage medium based on business needs. This approach enhances storage utilization and reduces storage acquisition costs. Compliance with legislation is another important factor in determining how organizations handle data lifecycle, retention, and archiving. It's important to note that archiving and backup are not synonymous. Archiving involves removing a file from the source and replacing it with a pointer to retrieve it from the archive. On the other hand, backup provides temporary data protection by copying a large block of data to secondary storage.

By considering the data lifecycle, storage optimization, compliance requirements, and appropriate data management practices, organizations can effectively govern their data assets and ensure their availability, integrity, and security throughout their lifecycle.

The next table present a pragmatic outlook on research themes for data governance in organizations [9]:

	Theme 1 Embracing data governance without compromising digital innovation	Theme 2 Enacting data governance through repertoires of mechanisms	Theme 3 From data governance to governing data	Theme 4 From systems to data to services
Practical issue	Organizations often emphasize data protection at the expense of data-driven value creation. This leads to perceptions that data governance hinders rather than enables digital innovation.	Data governance frameworks are presented as generic programs, but the enactment of data governance varies widely across organizations and contexts.	Data governance is often viewed as series of mechanisms implemented in organizations, at the expense of understanding the process of governing data.	Many organizations still conceive data as assets “at rest” in systems. Being able to innovate with data while protecting data requires engaging with the nature of data as assets *in flux*.
Relevance	Data governance aims at leveraging data to create value while ensuring its protection; maintaining a balance between these two seemingly contradictory objectives is challenging.	The duality of data governance, coupled with its contingent nature, require different combinations of mechanisms to protect data while fostering digital innovation.	The design of data governance only provides a partial account of data governance in an organization; the instantiation of this design in practice is important to understand how an organization protects and leverages data for digital innovation.	Organizations traditionally adopt a view of data based on the existence of physical and/or functional silos. Data-based digital innovation requires the removal of those silos, or at least the ability for data to seamlessly across those silos.

	Theme 1 Embracing data governance without compromising digital innovation	Theme 2 Enacting data governance through repertoires of mechanisms	Theme 3 From data governance to governing data	Theme 4 From systems to data to services
Relevance of data governance mechanisms	Structural mechanisms (e.g., security and access policies) are traditionally perceived as restrictive, while the potential for procedural mechanisms (e.g., data dictionaries, data lineage facilities) as well as relational mechanisms (e.g., employee coaching) to balance the dual objectives of data governance remains understudied.	Accounting for the relative contributions of each type of governance mechanisms to the achievement of both objectives of data governance is important to uncover and understand patterns of structural, procedure, and relational data governance mechanisms.	Data governance mechanisms are traditionally planned but studying their enactment in practice is important to understand their contributions to the dual objectives of data governance (e.g., employee coaching—a relational mechanism—may foster better alignment with policies and guidelines that exist as structural mechanisms).	Current trends emphasize the importance of services to enable data-based digital innovation. The provision of those services relies on structural, procedural, and relational mechanisms (e.g., dynamic access quotas, best practices) that depart significantly from the more traditional view of IT governance based on the existence of physical IT artifacts.
Potential practical solution	Implement data governance mechanisms that are designed with the explicit goal of balancing data protection and digital innovation (e.g., when defining the roles and responsibilities of data stewards).	Build data governance profiles to help an organization determine how it fares based on its own objectives, but also to compare itself to other organizations for benchmarking purposes.	Consider implementing data governance mechanisms in an iterative manner, within the context of data-driven initiatives to ensure that those mechanisms are quickly evaluated and adjusted if needed.	Implement digital services embedding procedural mechanisms (e.g., via APIs) that are consistent with data governance requirements for the organization.
How IS research can help	Research can draw attention to the possibility to espouse the two objectives of data governance as paradoxical, fostering the implementation of mechanisms (e.g., data stewards) that can help to reconcile both objectives.	Research can help to develop a conceptualization of data governance as repertoires of mechanisms that form configurations that contribute to the achievement of organizational outcomes.	Like strategy, data governance incorporates both planned and emergent components, calling for approaches that are closer to the practice of governing data and its impact on everyday work.	Research provides the conceptual scaffolding and the empirical evidence supporting an approach to governing data based on the provision and the orchestration of digital services.

	Theme 1 Embracing data governance without compromising digital innovation	Theme 2 Enacting data governance through repertoires of mechanisms	Theme 3 From data governance to governing data	Theme 4 From systems to data to services
Potential conceptual foundation(s)	Paradoxes and tensions; Paradoxical thinking (e.g., Gaim, Wåhlin, Pina e Cunha, & Clegg, 2018; Lewis, 2000; Poole & Van de Ven, 1989; Putnam, Fairhurst, & Banghart, 2016; Quinn & Cameron, 1988)	Taxonomies (Nickerson, Varshney, & Muntermann, 2013; Oberl¨ander, R¨oglinger, & Rosemann, 2021); Typologies (e.g., Doty & Glick, 1994; Gregor, 2006)	Practice perspective (e.g., Jarzabkowski, L, & Feldman, 2012; Peppard, Galliers, & Thorogood, 2014); **Ostensive and performative aspects of organizational elements** (e.g., Latour, 1986) **and routines** (e.g, Feldman & Pentland, 2003);	Orchestration (e.g., Maruping & Matook, 2020); **Servitization** (e.g., Schüritz, Seebacher, Satzger, & Schwarz, 2017)

c) The contribution of IT audit to data governance for Moroccan SMEs

IT audit can bring several beneficial perspectives to data governance for Moroccan SMEs. Here are some key points :

Compliance assessment: IT audit examines the policies and procedures in place for data management in Moroccan SMEs. It ensures that data collection, storage, processing, and sharing practices comply with current laws and regulations, such as the Moroccan law on personal data protection. The audit identifies any non-compliance and recommends corrective actions as necessary.

Data security audit: IT audit assesses data security within SMEs. This includes identifying potential vulnerabilities in systems and networks, evaluating existing security controls such as data access and mechanisms for protecting sensitive data. The audit recommends appropriate security measures to ensure data confidentiality, integrity, and availability.

Data management process evaluation: IT audit examines data management processes in Moroccan SMEs, from collection to archiving. It assesses the effectiveness of existing processes, identifies bottlenecks and inefficiencies, and proposes improvements to optimize data flows, reduce errors, and ensure data quality.

Data quality evaluation: IT audit assesses data quality within Moroccan SMEs. This includes evaluating the accuracy, relevance, consistency, and completeness of data. The audit identifies gaps in data quality and recommends measures to improve reliability and accuracy of data used by the organization.

Awareness and training: IT audit can contribute to raising awareness among employees of Moroccan SMEs about the importance of data governance and train them in best practices. This may include training sessions on data management, data security, privacy protection, and regulatory compliance. This awareness reinforces the data governance culture within the organization and promotes responsible data usage.

In summary, IT audit provides a comprehensive evaluation of data governance in Moroccan SMEs, covering aspects such as compliance, security, data quality, and management processes. It provides practical recommendations to enhance data governance, strengthen security, and ensure compliance with legal and regulatory requirements.

Conclusion:

Information systems are a fundamental part of every organization, they exist a lot of security techniques to protect information systems form risk, the use of any of this security techniques should be based on the nature of the potential risks, in a way to guarantee properly and effective protection to the organization assets and data. The internal and external security audit is best way to ensure the security efficiency.

Data governance can be considered more than its concept in the conclusion of this research. With the implementation of Data governance, companies will be able to consolidate collaborative management paradigms to share, exchange and transfer data from the organizational level to the inter-organizational level and learning networks.

According to this line of reasoning, it's essential to choose an enterprise governance structure that promotes collaboration and sharing at multiple levels in the data generation process. To positively influence the processes of knowledge transfer, sharing and creation, it's necessary to define governance and coordination mechanisms.

Acknowledgment:

We thank all our colleague for their valuable help and comments.

Bibliography

1. Khatri, V. & C.V. Brown (2010). Designing data governance. Communications of the ACM
2. S. Anantha Sayana, CISA, CIA "The IS Audit Process" Information Systems Control Journal, Volume 1, 2002
3. ISACA (2012) COBIT 5 - A Business Framework for the Governance and Management of Enterprise IT
4. D. Drljača, B.Latinović "Frameworks For Audit Of An Information system In Practice"Journal of Information Technology and Applications, 2016
5. M. Gheorghe, "Audit Methodology for IT Governance ", Informatica Economică vol. 14, no. 1/2010
6. Ning Zhang, Qin jianYuan An Overview of Data Governance
7. Alpha Males and Data Disasters: the Case for Data Governance. Brass Cannon Press Thomas, G (2006).

8. Ladley J. (2012). Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program. Newnes.
9. Gregory Vial Data governance and digital innovation: A translational account of practitioner issues for IS research