# DO REGULATORS PAY ATTENTION? AN ASSESSMENT OF IT GOVERNANCE IMPLEMENTATION IN SYSTEMICALLY IMPORTANT BANKS

Mehrdad Sepahvand *, Homa Monfared *

* Monetary and Banking Research Institute, Tehran, Iran

OPEN ACCESS

**How to cite this paper:** Sepahvand, M., Monfared, H. (2017). Do Regulators Pay Attention? An Assessment of IT Governance Implementation in Systemically Important Banks. *Journal of Governance and Regulation, 6(1), 90-99.* http://dx.doi.org/10.22495/jgr_v6_i1_p8



**ISSN Online:** 2306-6784
**ISSN Print:** 2220-9352

**Received:** 10.01.2017
**Accepted:** 15.03.2017

**JEL Classification:** G2, G3, O32
**DOI:** 10.22495/jgr_v6_i1_p8

## Abstract

The large size and complexity of Information Technology systems in systematically important banks raise the need for creating an IT governance architecture that could make IT strategy aligned with business strategy and delivers value while it effectively identifies and manages IT risk. This study traces the links between IT governance and two more applied risk management frameworks, COSO and BCBS's principles for managing IT risk. Then it argues due to the magnitude of potential losses caused by any weakness in IT governance in D-SIBs, the assessment of IT governance in these banks should be one of the main concerns of local regulators and supervisors. As a case study, it assesses the relative rank of D-SIBs in Iranian banking system to see where these banks would stand in an ordered list of the banks including both private and public banks in terms of IT governance implementation. The application of the Fuzzy AHP technique shows that IT governance practice in Iranian D-SIBs is not as good as the private banks while it outperforms some state-owned banks.

**Keywords:** IT Governance, Systematically Important Banks, IT Risk, Fuzzy AHP

## 1. INTRODUCTION

Nowadays, Information Technology (IT) has become crucial to the banking business survival in a competitive environment and to achieve business continuity in this industry all around the world. This is quite understandable as banking is an information-intensive industry and therefore IT has a great role to play in empowering the business with managing customer's information, developing effective business processes and also to open new channels to deliver services. In fact, an updated and well-organized IT infrastructure is no longer a "nice to have", but a "must have" ingredient of the banking business. Without the power of technology based systems, it would not be possible for banks to store and retrieve huge amounts of customer data, transaction data and business information. It is also vital for continuity of banking business to adopt an updated IT system that enables the bank to be innovative and respond quickly to its customers evolving needs in a timely manner; that is to say IT is essential for being customer-centric. Finally, banks are increasingly using IT-based platforms and applications to support decision-making and monitoring and also to respond to compliance requirements. That is not all, the big changes is yet to come; information technology paves the way to digitalization which definitely will revolutionize banking in future.

While the utilization of IT in banking business has its own benefits, such IT usage and dependence, however, bring in some new challenges and concerns for both bankers and supervision authorities. From bankers' point of view, there are a number of concerns including security of information systems and management of IT investments. In the IT age, not only being innovative is equal to be digitalized, but the trust in banks is particularly synonymous with trust in IT. In particular, operational risk in IT and the threat of cyber-attacks have become increasingly important. A global study conducted in 2015 revealed that 61% of CEOs believe that cyber risks present a key threat. In this study, financial institutions were ranked first out of all sectors in 2014 as the main purchasers of insurance against cyber risks with average limits of USD57 million (Dombret, 2016).

The vast use of new technology in banking brings in the challenges of dealing with large-scale IT projects with long-term time span. As it has been outlined in G-30 document, "given that for many

large firms, necessary investments will run to several billion dollars over the coming years, boards may need to rethink their approach to evaluating management's investment in core IT spending." There are many questions that senior bank managers struggle with: Is the project in line with the enterprise business strategy and brings value to the bank? Is the IT department capable of handling the investment project in a cost-efficient and timely manner? Then we come to a more general question that if bank could develop a framework to ensure the effectiveness and efficiency of IT spending.

Regulators and Supervisors are faced with the challenge of overseeing very sophisticated information systems. They cannot easily rely on the collected risk information from different business segments and different geographical locations in a timely and comprehensive manner unless banks are enjoying a robust and effective IT system. Recently, released guidelines of Basel Committee on Banking Supervision (BCBS) on corporate governance principles for banks highlights the significance of knowledge of information technology and related risks for board members. The new guideline also recommends banks to develop a sufficiently robust data infrastructure, data architecture and information technology infrastructure which adequately correspond to their IT system's sophistication (BIS, 2015).

IT governance simply embraces and addresses all the above challenges. IT governance involves managing IT operations and IT projects to ensure alignment between these activities and the needs of the organization defined in the strategic plan. IT governance is integral part of organizational management and responsibility of managing and supervising boards and it consists of leadership, organizational structure and processes that ensure IT is used to enhance the value of the organization. That is the role of internal audit for IT governance to ensure the management board of implementing IT governance processes and structures.

One of the main lessons learned from the financial crisis of 2007–08 was that banks cannot be treated equally by regulators. There are some banks, normally with a big size that if those banks fail, they jeopardize the stability of the whole system. These banks are known as Systematically Important Banks (SIBs) and the Financial Stability Board (FSB) of Bank for International Settlement (BIS) has developed a method to identify SIBs in order to apply stricter regulatory requirements to these banks since 2009. In response to this regulatory need, in some countries the banking authorities created a 'large institution supervision coordinating committee' framework tasked with overseeing the supervision of the largest, most systemically important financial institutions. While size is one of the main determinant to identify SIBs, it has been proven empirically that organization size influences IT sophistication of the organization (Lehman, 1985). Laeven et al. (2014) investigates the relationship between size, complexity of organization and systemic risk in banking business. He relies on an empirical analysis to show large banks, on average, create more individual and systemic risk than smaller banks.

Despite the growing interest in systematically important banks' regulation and the significance of IT governance in this type of banks, to the best of our knowledge, no previous research has been reported which directly deals with the assessment of IT governance in SIBs. This paper is trying to fill the gap by addressing the need for IT governance assessment in the SIBs in the Iranian banking system. More specifically, this study compares IT governance implementation in local systematically important banks introduced by Sepahvand and Heidari (2015) with other privately-owned and those banks that are controlled by government that are operating in the Iranian banking system. The banks performance are assessed in all 5 focused areas of IT governance to see in which area the gap between SIBs and other banks performance is wider and therefore SIBs are more in need for taking some corrective action.

This study is organized as follows. Section 2 introduces the focus areas of IT governance and uses the COBIT process to connect that with the regulatory principles for governance risk and IT risk as a Part of operational risk management. Section 3 deals with D-SIBs and some common features including large size and high complexity that urge the implementation of IT governance and the application of some auditing procedures. Then the D-SIBs in Iranian banking system are introduced. The methodology of assessment is explained in Section 4 and finally Section 5 concludes.

## 2. IT GOVERNANCE AND OPERATIONAL RISKS

The regulators' concerns over banks and credit institutions' appropriate management of information system and IT projects have been reflected in two sets of principles issued by BCBS of BIS, namely corporate governance principles and operational risk management principles. Harun R Khan refers to this dichotomy as concerns over IT strategy on one hand and the way that one operationalizes the strategy on the other hand (Khan, 2015).

The relationship between corporate governance and IT governance is straightforward. IT governance as subcategory of corporate governance has its specificities and is of crucial importance to banks in order to keep performing their business activities by minimizing risks and accomplishing their full potential. But bank managing and supervisory boards often remain uncertain how to assess their IT governance, effects it has on bank and areas that need improvement (Lacković, 2013). Therefore the principles are introduced by regulatory agencies based on best practices to promote banks performance in this area. Perhaps the Sarbanes-Oxley Act of 2002 (SOX) of the United States was the first state intervention on corporate governance practices wherein as a part of self-assessment, financial institutions including banks are required testing of IT general controls, checking IT process element at the time of each period-end financial reporting, examining the IT process flow control of actual transactions and finally measuring the effectiveness of IT general controls over financial reporting (Anand, 2012). Recently released guidelines of Basel Committee on Banking Supervision (BCBS) on corporate governance principles for banks highlights the board members having knowledge, relating to role of information technology in risk governance. The guidelines also prescribe that the degree of sophistication of the

bank's risk management infrastructure – including, in particular, a sufficiently robust data infrastructure, data architecture and information technology infrastructure – should keep pace with developments such as balance sheet and revenue growth; increasing complexity of the bank's business, risk configuration or operating structure; geographical expansion; mergers and acquisitions; or the introduction of new products or business lines (BIS, 2015).

Requirements of Basel II and Basel III related to information systems are related to emphasize on importance of IT risk as a part of operational risk system. The Basel Committee has defined the operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". As the main part of operational Risk, the IT risk is defined by the Information Systems Audit and Control Associations - ISACA as a business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise (ISACA, 2009). BCBS has issued in 2003 the "Sound Practices for the Management and Supervision of Operational Risk" document, which provides a framework for the effective management and supervision of operational risk. Operational risk management is a process with two main components, identification and control. First part means to identify vulnerabilities and threats to the information resources used for achieving the business objectives and the second one, to decide, based on the value of the information resource for the business, what countermeasure to take in reducing risks to an acceptable level. As the IT risk is an important part of the operational risk, the 10 principles recommended in this document are relevant to IT risk as well. IT risk management is the cornerstones of the information system auditing regulation that obliged every bank and credit institution to perform internal and especially external assessment of IT risks and to prepare a report for the regulator as well as for company's Board.

The ten Basel II principles could be grouped under the following categories:

Establishing an appropriate risk management framework– This category covers principles (1-3) and includes board awareness and approval process, introducing appropriate internal auditing process and establishing the risk management framework.

Offering guidance over the risk management process – This category covers principles (4-7) and includes identification and assessments process, defining the operational risk monitoring process, periodically review of the risk management policies, processes and control strategies and finally having contingency and business continuity plans.

The role of supervisors – This includes principles 8 and 9 which deal with banking supervision requirements for effective framework and regular independent evaluation of a bank's policies, procedures and practices related to operational risks.

Disclosure – The last principle deals with establishing the public disclosure of information by the banks.

IT Governance is a fairly new concept as a defined discipline and is still evolving. According to ITGI, IT governance is 'a set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly'(Global Technology Audit Guide, 2012). IT Governance is not just an IT issue or only of interest to the IT function. In its broadest sense it is a part of the overall governance of an entity, but with a specific focus on improving the management and control of Information Technology for the benefit of the whole organization. IT Governance spans the culture, organization, policy and practices that provide for IT management and control across five key areas:

Alignment – Provide strategic direction of IT and the alignment of IT and the business with respect to services and projects.

Value Delivery – Confirm that the IT/Business organization is designed to drive maximum business value from IT. Oversee the delivery of value by IT to the business, and assess ROI.

Risk Management – Ascertain that processes are in place to ensure that risks have been adequately managed. Include assessment of the risk aspects of IT investments.

Resource Management – Provide high-level direction for sourcing and use of IT resources. Oversee the aggregate funding of IT at enterprise level. Ensure there is an adequate IT capability and infrastructure to support current and expected future business requirements.

Performance Measurement – Verify strategic compliance, i.e. achievement of strategic IT objectives.

There are some other frameworks that are concerned with the management of operational risk and governance of information systems. These frameworks normally have a broad coverage and operational risk management including IT risk management is only part of their objectives. Two most applied frameworks are COSO and COBIT that will be explained shortly.

The "Control Objectives for Information and related Technology" – COBIT framework, issued by the IT Governance Institute (ITGI, 2007), is a comprehensive framework for the management of IT risk and control, which provides a set of IT processes and controls suited to address the Basel II requirements related to information risk management. COBIT has a business orientation, linking business goals to IT goals, providing metrics and maturity models for their accomplishment and identifying accountability for business and IT process owners. COBIT may assist in defining a standardized control environment by stating the applicable control processes. COBIT IT processes that have the same problem is organized into a domain. COBIT Framework is made of four main domains, namely:

Planning & Organization – This domain is more likely to concern on planning and organizing process of IT and enterprise strategies.

Acquisition & Implementation – This domain connects with selection, procurement, and applied IT used in the enterprise.

Delivery & Support – This domain is mainly about IT service processes and its technical supports.

Monitoring & Evaluation – This domain concerns on IT security process in the organization.

The internal control framework issued by Committee of Sponsoring Organizations (COSO) in 1985 introduces some criteria for determining the effectiveness of an internal control system. The COSO internal framework comprises five areas of interests which cover the activity of the managers in charge with the business:

Control environment – This issue sets the framework for the action of all the other components of internal control. Control environment factors comprise the integrity, ethical values, and delegation of authority as well as the management's operating style in relation with entity's human resources.

Risk assessment – The entity encounters many risks from inside or outside of the organization. Such risks should be appraised and assumed. Risks are related with the objectives of the organization and in this context risks should be assessed.

Information and communication – This issue ensures the information circuit within the framework of organization and permits the exchange of feedback.

Control activities – This issue covers the policies implemented to ensure the pursuing of the management directives. Such controls assure that necessary actions are taken to avoid risks that threat the achievement of current objectives.

Monitoring – This issue addresses the assessment of the system's performance over time. Through this process the weaknesses of internal control are detected and analyzed in order to correct them and improve continuous the system's behavior.

Table 1 shows the mapping relationship between the IT governance focus area, regulatory Basel II principles, COSO components and COBIT4 main domains and processes. It shows the relationship between IT process, IT resources and operational risk management criteria.

The table consists of 4 main columns. The first three columns of the table are borrowed from Appendix II of COBIT4 (ITGI, 2007) while the forth one uses the mapping that is driven from Basel principles classified in four main domains given in the first part of the section plus a related item from corporate governance principles. The importance values (P is used for primary and S is used for secondary relations) in the first three columns are based on a survey run by ITGI and the value for the last column is estimated using the opinion of some experts and are provided only as a guide as mentioned in the ITGI document's Appendix. As noticed by (Nastase and Unchiasu, 2013) in the above table, many COBIT processes have relationship with more than one Basel II principle, due to the nature of general IT control. This multiple relationship expresses the importance of IT controls for a reliable internal control system. In Table 1, COBIT IT processes are used as matching tools to establish the connection between IT governance and Basel II principles.

## 2.1 Operational Risks and D-SIBs

It was the recent global financial crisis that urged the regulators and policymakers to find new ways to address systemically important financial institutions. Before this event, although the significance of SIBs was underscored, no special treatment for such institutions had been applied by regulators and supervisors around the world. Since then, the Financial Stability Board applies the BCBS methodology that makes use of accounting and supervisory data as proxies of five main characteristics (size, interconnectedness, substitutability of services, complexity, and cross-jurisdictional activity that can be theoretically related to systemic importance) to identify SIBs in each jurisdiction. The Basel Accord also requires the banks to implement policies, procedures and practices to manage operational risk commensurate with their size, complexity, activities and risk exposure.' (BCBS 2014, p. 4).

As mentioned above size and complexity are two factors that also affect the operational risk of the banks. Some researches point to tradeoff between potential synergies and diversification benefits from a financial institution's involvement in multiple business lines versus the potential risk management weaknesses generated by their increased complexity that can result in potential losses. Goetz et al. (2014) find that geographic diversification reduces a bank's risk, while Focarelli et al.(2011) show that those firm that borrow from large banks are more likely to default. Chernobai et al. (2016) contribute to this debate by studying the effects of business diversification on operational risk events and comparing them with the effects on market-based and balance-sheet-based performance measures, such as market-to-book value and the mean and standard deviation of return on assets. Following Buffa (2016), they show that, while these performance measures typically improve after deregulation for banks that were constrained by the financial regulations, in general the operational risk of these banks goes up (Chernobai et al., 2016).

There have been few published works directly addressing the linkage between complexity, systemic risk and operational risks. Gai, et al. (2011) studied a network model of interbank lending and showed how greater complexity and concentration in the financial network amplifies systemic risk. Moosa (2006) in his study "Misconceptions about operational risk" (2006) claims that systemic risk could be triggered by operational risks.

If the D-SIDs are deemed to be more exposed to operational risks and IT risk in particular, we may expect these banks to be equipped with a more developed IT governance framework to deal with IT strategy and IT risk. In the next part of this study we try to verify this claim using field data.

## 2.2 D-SIBs in Iranian Banking System

Iran is the second largest country in Middle East and the 17th country in the world in term of GDP in purchasing power parity scale. The Iranian financial system is bank-based and government has still a large stake in the economy and the banking system. By 2016, some 32 banks (28 commercial and 4 specialized) with about 22000 branches were in operation. Since 2001, the government began to privatize the banking sector and licenses were issued to some new privately owned banks. Of 2016, the banking system was composed of 6 state-owned (including Bank Melli) along with 28 private banks from which four large banks including Bank Mellat are newly privatized and still controlled by government.

**Table 1.** Mapping IT Processes from COBIT4 to Basel II Principles, IT Governance and COSO Components

| | IMPOR-TANCE | IT Governance Focus Areas | | | | | Coso | | | | | Operational Risk-Basel Framework | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Strategic Alignment | Value Delivery | Resource Management | Risk Management | Performance Measurement | Control Environment | Risk Assessment | Control Activities | Information and Communication | Monitoring | Corporate Governance | Establishing an appropriate risk management framework | Offering guidance over the risk management process | The role of supervisors | Disclosure |
| Plan and Organize | | | | | | | | | | | | | | | | |
| PO1 Define a strategic IT plan. | H | P | | S | S | | | P | | S | S | P | | | | |
| PO2 Define the information architecture. | L | P | S | P | S | | | | P | P | | | P | | | |
| PO3 Determine technological direction. | M | S | S | P | S | | | S | P | S | | P | | | | |
| PO4 Define the IT processes, organization and relationships. | L | S | | P | P | | P | | | S | S | | P | P | S | |
| PO5 Manage the IT investment. | M | S | P | S | | | | S | P | | | S | | | | |
| PO6 Communicate management aims and direction. | M | P | | | P | | P | | | P | | | | | | P |
| PO7 Manage IT human resources. | L | P | | P | S | | P | | | S | | S | S | | | |
| PO8 Manage quality. | M | P | S | | S | P | P | | P | S | P | | | | | |
| PO9 Assess and manage IT risks. | H | P | | | | | | P | | | | S | | P | P | |
| PO10 Manage projects. | H | P | S | S | | S | S | S | P | | S | | S | | | |
| Acquire and Implement | | | | | | | | | | | | | | | | |
| AI1 Identify automated solutions. | M | P | P | S | S | | | | P | | | | S | | S | |
| AI2 Acquire and maintain application software. | M | P | P | | S | | | | P | | | | | | | |
| AI3 Acquire and maintain technology infrastructure. | L | | | P | | | | | P | | | S | | | | |
| AI4 Enable operation and use. | L | S | P | S | S | | | | P | S | | | | | | |
| AI5 Procure IT resources. | M | | S | P | | | | | P | | | | | | | |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AI6 Manage changes. | H | | P | S | | | | S | P | | S | S | | | S | |
| AI7 Install and accredit solutions and changes. | M | S | P | S | S | S | | | P | S | S | | | | | |
| Deliver and Support | | | | | | | | | | | | | | | | |
| DS1 Define and manage service levels. | M | P | P | P | | P | S | | P | s | s | | P | | | |
| DS2 Manage third-party services. | L | | P | S | P | S | P | S | P | | s | | | | | |
| DS3 Manage performance and capacity. | L | S | S | P | S | S | | | P | | s | | | | | |
| DS4 Ensure continuous service. | M | S | P | S | P | S | S | | P | s | | | S | S | | |
| DS5 Ensure systems security. | H | | | | P | | | | P | s | s | P | P | | P | |
| DS6 Identify and allocate costs. | L | | S | P | | S | P | | P | | | | | | | |
| DS7 Educate and train users. | L | S | P | S | S | | S | | | s | | | | | S | |
| DS8 Manage service desk and incidents. | L | | P | | | S | | | | p | p | | | | | |
| DS9 Manage the configuration. | M | | P | P | S | | | | P | | | | | S | S | |
| DS10 Manage problems. | M | | P | | S | S | | | P | s | s | | S | S | | |
| DS11 Manage data. | H | | P | P | P | | | | P | | | | S | S | P | |
| DS12 Manage the physical environment. | L | | | S | P | | | S | P | | | | | S | S | |
| DS13 Manage operations. | L | | | P | | | | | P | s | | | S | | S | |
| Monitor and Evaluate | | | | | | | | | | | | | | | | |
| ME1 Monitor and evaluate IT performance. | H | S | S | S | S | P | | | | S | P | P | S | | S | P |
| ME2 Monitor and evaluate internal control. | M | | P | | P | | | | | | P | P | S | | | |
| ME3 Ensure compliance with external requirements. | H | P | | | P | | | | P | S | S | | | | P | |
| ME4 Provide IT governance. | H | P | P | P | P | P | P | S | | S | P | P | P | S | P | S |

Very little work has been reported on systemic risk and identifying systemically important banks in Iranian banking system. Regarding the measurement of systemic risk, Sepahvand and Banitorof (2014) used the interbank transaction data to see if the magnitude of systemic risk before the launch of RTGS was significant enough to justify the costs of such a radical change in payment infrastructure.

To identify the D-SIBs, Sepahvand and Heidari (2015) used the indicator-based approach suggested by international regulatory agencies along with an alternative approach that mainly relies on network properties such as degree, strength, between ess, closeness and pagerank. Appling a fuzzy c-mean clustering method they found that the results from both approaches are comparable. Their results indicated that two large banks namely Bank Melli and Bank Mellat appeared to be D-SIBs in the local banking system.

Bank Melli Iran (BMI) is the first national Iranian bank and was established in 1927 by constitution. BMI is now the largest commercial retail bank in Iran and even in the Middle East with over 3,300 branches both inside and outside of the country and with 43,000 employees. The Bank is owned and operated by the government of Iran. It has equity share directly in around 37 companies that are scattered from construction industry to investment management business. The share of BMI of the total deposits of the banking sector amount to 20 percent while the number of employees of BMI was 29 percent of the total employment of the banking sector in 2015.

Bank Mellat (BM) is a private bank by virtue of its capital ownership however, the government still have control over the bank management. BM was established in 1980 by merging ten pre-revolution private banks including Tehran, Dariush, Pars, Etebarat Taavoni & Tozie, Iran & Arab, Bein-al-melalie-Iran, Omran, Bimeh Iran, Tejarat Khareji Iran and Farhangian banks. Currently, the bank's capital amounts to Rls 13,100 billion and it is one of the largest commercial banks in the Islamic Republic of Iran, ranking among the top 1000 banks of the world.

## 3. ASSESSMENT METHODOLOGY

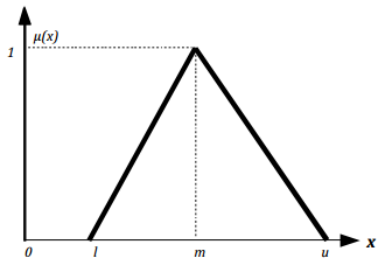
The aim of this study is to assess the relative rank of D-SIBs to see where these banks would stand in an ordered list of the banks including both private and public banks in terms of IT governance implementation. The ranking is developed through the Analytic Hierarchy Process (AHP) methodology following Cobo et. al. (2015) with IT governance as the goal of our analysis and each domain of IT governance appears in the role of a criteria for assessment of different type of banks as our alternatives. As the traditional AHP method is problematic due to the fact that it uses the exact values to express the decision maker's opinion despite of the inherent uncertainty and imprecision in the pairwise comparison process in a comparison of alternatives, a Fuzzy AHP (FAHP) is applied for solving the hierarchical rating problem. Then the results of rating would be used as a base for ranking purpose.

The simplest fuzzy numbers are triangular fuzzy numbers. A triangular fuzzy number is a special type of fuzzy number whose membership is defined by three real numbers, expressed as *(l, m, u)*, where *l* is the lower limit, *m* the most promising and *u* the upper limit value. The membership function of *M=(l,m,u)* is given by:

$$\mu(x)=\begin{cases}\frac{x-1}{m-1} & if \quad l \le x \le m \\ \frac{x-u}{m-u} & if \quad m \le x \le u \\ 0 \quad if & x < l \ or \ x > a\end{cases} \tag{1}$$

The graphical representation of this function can be seen in Figure 2.

**Figure 1**. Membership function defining the triangular fuzzy number M=(a,b,c).




The fuzzy numbers required to form the decision matrix may be determined directly according to the decision maker or may derive from linguistic variables in a verbal scale, which can be then converted into fuzzy numbers using a suitable conversion as shown in Table 2. In order to construct a positive reciprocal matrix of pairwise comparisons, a full set of *n(n-1)/2* comparison judgments are required. The pairwise comparison matrix is constructed as

$$A=\begin{pmatrix}\tilde{1} & \tilde{a}_{12} & \dots & \tilde{a}_{12} \\ \tilde{a}_{21} & \tilde{1} & \dots & \tilde{a}_{2n} \\ & & \cdot & \\ & & \cdot & \\ & & \cdot & \\ \tilde{a}_{n1} & \tilde{a}_{n2} & \dots & \tilde{1}\end{pmatrix} \tag{2}$$

where $\tilde{a}_{ij}=(l_{ij}, m_{ij}, u_{ij})$ and $\tilde{1}=(1,1,1)$ and $\tilde{a}_{ji}=1/\tilde{a}_{ij}$.

**Table 2.** Fundamental Scale

| FAHP: Fuzzy number | AHP: Crisp number | Intensity of Importance of one criterion over another |
|---|---|---|
| [1 1 1 ] | 1 | equally important |
| [2/3 1 3/2] | 3 | moderate importance of one over another |
| [3/2 2 5/2] | 5 | strong or essential importance |
| [5/2 3 7/2] | 7 | very strong demonstrated importance |
| [7/2 4 9/2] | 9 | extreme importance |
| [1/2 3/4 1 ] , [1 3/2 2] , [2 5/2 3 ] , [3 7/2 4 ] | 2,4,6,8 | immediate values |

The final weights of the decision elements can be calculated using different methods that have been proposed in the literature. One of the most popular methods is the Fuzzy Extent Analysis, proposed by Chang (1996). The steps of Chang's extent analysis can be summarized as follows:

First step: computing the normalized value of row sums by fuzzy arithmetic operations:

$$\tilde{S}_i = \sum_{j=1}^{n} \tilde{a}_{ij} * \left( \sum_{k=1}^{n} \sum_{j=1}^{n} \tilde{a}_{kj} \right)^{-1} \quad (3)$$

Second step: computing the degree of possibility of $\tilde{S}_i \geq \tilde{S}_j$ defined as

$$V(\tilde{S}_i \geq \tilde{S}_j) = sup_{y \geq x}[\min(\tilde{S}_j(x), \tilde{S}_i(y))] \quad (4)$$

$x$ and $y$ being the values on the axis of the membership function of each criterion. This expression is equivalently expressed as

$$V(\tilde{S}_i \geq \tilde{S}_j) = \begin{cases} 1 & if \quad m_i \geq m_j \\ \frac{u_i - l_j}{(u_i - m_i) + (m_j - l_j)} & if \quad l_j \leq u_i \\ 0 & otherwise \end{cases} \quad (5)$$

Where $\tilde{S}_i = (l_i, m_i, u_i)$ and $\tilde{S}_j = (l_j, m_j, u_j)$. Using these expressions the degree of possibility of to be greater than all the convex fuzzy numbers is computed as follows:

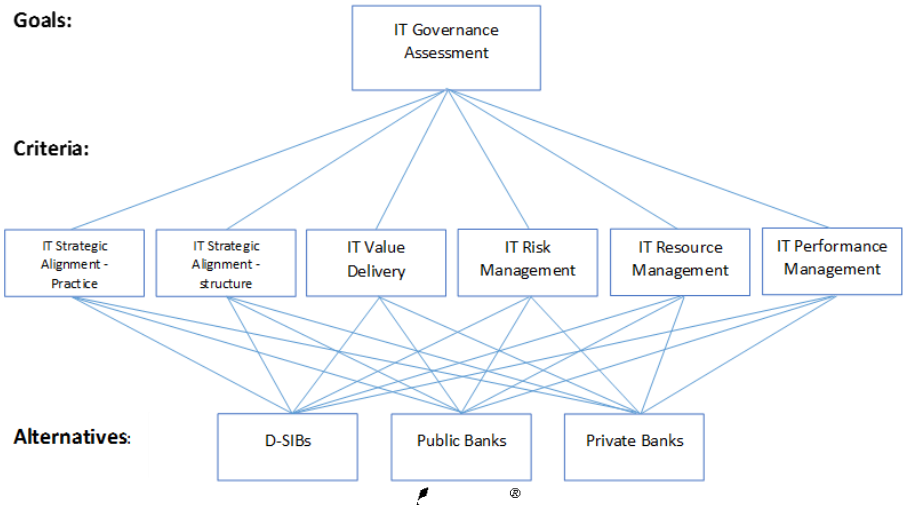
$$V(\tilde{S} \geq \tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_n) = \min V(\tilde{S} \geq \tilde{S}_k) \quad (6)$$

Third step: defining the priority normalized vector of the fuzzy comparison matrix as:

$$w_i = \frac{V(\tilde{S}_i \geq \tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_n)}{\sum_{k=1}^{n} V(\tilde{S}_k \geq \tilde{S}_1, \tilde{S}_2, \ldots, \tilde{S}_n)}; \quad i = 1,2, \ldots, n \quad (7)$$

As mentioned above, in this study IT governance is set as the goal of our analysis and each domain of IT governance appears in the role of a criteria for assessment of different type of banks as our alternatives. In the first level of the criteria hierarchy, we consider the six main domains $D_i$, $i=(1,2,3,4,5,6)$ where $D_1$ corresponds to "IT strategic alignment Practice ", $D_2$ is "IT strategic alignment Structure ", $D_3$ is "IT value delivery" and $D_4$ is "IT risk management", $D_5$ is "IT Resource management" and $D_6$ is "IT performance management". At the alternatives level we have three categories $A_i=(1,2,3)$ where $A_1$ is D-SIBs, that includes BMI and BM, $A_2$ is "Public banks" including 6 specialized banks, Sepah bank and three newly privatized banks and the rest are grouped as "Private Banks". It worth to know the newly privatized banks are still under the state control so they are included in Public Bank's category.

**Figure 2.** The elements of Analysis Hierarchy



A pairwise comparison is conducted by 26 people who were working in IT departments at senior management level with at least ten years work experience. The participants in the survey were contacted through web-questionnaires with 35 close ended questions. We have checked the consistency of comparative judgments between domains at the criteria level, using the ratio of consistency recommended by Saaty (1980). It is recommended the radius of consistency to be 0.1 or lower so that pairwise comparisons undertaken by the decision maker can be considered as acceptable. In this study the values obtained for the two levels of the hierarchy were of 0.07 for the first level and for the second level comparisons, we obtained radius of consistency of 0.05, 0.05, 0.5, 0.05, 0.05, and 0.001 respectively. All ratios of consistency were, therefore, perfectly admissible.

The pairwise comparisons matrix (2) is calculated for the all criteria and presented in Table 3.

**Table 3**. Reciprocal Matrix of Pairwise Comparisons

| | **IT Str. Algnt Pr** | **IT Str. Algnt Str** | **IT Value Delivery** | **IT Risk Mgt** | **IT Resource Mgt** | **IT Perf.Mgt** |
|---|---|---|---|---|---|---|
| IT Str. Algnt Pr | [1,1,1] | [2.5,3,3.5] | [1.5,2,2.5] | [0.66,1,1.5] | [0.5,0.75,1] | [1,1.5,2] |
| IT Str. Algnt Str | [0.28,0.33,0.] | [1,1,1] | [0.66,1,1.5] | [1.5,2,2.5] | [2,2.5,3] | [0.66,1,1.5] |
| IT Value Delivery | [0.4,0.5,0.66] | [0.66,1,1.5] | [1,1,1] | [0.5,0.75,1] | [0.66,1,1.5] | [0.66,1,1.5] |
| IT Risk Mgt | [0.66,1,1.5] | [0.4,0.5,0.66] | [1,1.33,2] | [1,1,1] | [0.5,0.75,1] | [2,2.50,3] |
| IT Resource Mgt | [1,1.33,2] | [0.33,0.4,0.5] | [0.66,1,1.5] | [1,1.33,2] | [1,1,1] | [0.66,1,1.5] |
| IT Perf.Mgt | [0.33,0.4,0.5] | [1,1.33,2] | [0.5,0.66,1] | [0.66,1,1.5] | [0.5,0.66,1] | [1,1,1] |

We also have calculated the pairwise comparison matrices for all alternatives in each criterion domain. By applying the FAHP methodology we can find the final rate for each alternative and the weights for each criterion which will influence the importance in achieving the final goal. The computation was performed using the Matlab software and the final ranking of alternatives with their rates are presented in Table 4.

**Table 4**. Final Results Based on FAHP Ranking

| **Levels** | **Ranking** |
|---|---|
| Weights and Ranking for IT Governance Criteria | IT- Str. Algn. Str > IT Risk Mgt. > IT- Str. Algn. Pr > IT Perf.Mgt. > IT Res. Mgt. > IT Value Delivery<br>(0.32) (0.25) (0.13) (0.11) (0.19) (0) |
| Ranking of different type of banks in ITG | Private > D-SIB > Public<br>(0.26) (0.24) (0.5) |

Table 4 prioritizes the criteria and alternatives in term of IT governance implementation. As it can be seen from the results, "IT strategic alignment Structure " and " IT Risk management ", have the highest priority in this assessment. At the first level "IT strategic alignment Practice" ranked third. The last item "IT Value Delivery" is assigned a null weight. The final results indicate that IT governance practice in Iranian D-SIBs is not as good as the private banks while it outperforms some state-owned banks.

## 4. SUMMARY AND CONCLUSION

The recent global financial crisis has urged the regulators and policymakers to find new ways to address systemically important financial institutions. The D-SIBs are identified by size and complexity which are two factors that also affect the operational risk of the banks. There have been few published works directly addressing the linkage between complexity, systemic risk and operational risks. However, it is quite understandable that the potential losses caused by any weakness in IT governance for D-SIBs could be magnificent in terms of its impact on the banking system. So the assessment of IT governance in these type of banks should be one of the main concerns of local regulators and supervisors.

There is a growing attention to IT risk in banking business and that is evident of the amount of money that banks are spending on managing IT risk and cyber-attacks in particular in large banking institutions around the globe. Banks use some IT control and risk management frameworks like COSO and COBIT to deal with IT risks. We have extended the mapping relationship between the IT governance focus areas, COSO components and COBIT4 main

domains presented in COBIT4 documents to regulatory Basel II principles of operational risk management in banking sector. Then we focused on D-SIBs characteristics to show why supervisors should be more vigilant on operational risk and IT governance for this type of banks in any jurisdiction.

The application of a Fuzzy AHP method in assessment of IT governance in D-SIBs in Iranian banking system revealed that the IT governance structure and practices in D-SIBs is not as good as their private counterparts. That could be of various reasons. First the migration from legacy systems in large banks is normally much more difficult and costly than that of small private banks. Also that could be attributed to the managerial slack or other problems that hinder the public enterprises efforts in dealing with structural changes.

Although this research reached its aim, there were some unavoidable limitations. The lack of reliable information and data constitutes a shortcoming of this study. The reliability of assessment depends on the reliability of the underlying information. There are some other source of information including financial and non-financial reports that are normally used in a professional assessment of IT governance in banking institutions. It is the task of the regulator to provide the banking system with the required protocols and standards in producing reliable data and information for supervision purposes. In fact, the lack of required information is mainly because of the supervisor negligence in producing such data. That forced us to rely only on a survey questionnaire with all known shortcomings.

## REFERENCES


1. Anand S. (2012). IT and Governance in Banks – Some Thoughts. BIS, Central bankers' speeches.
2. Basel Committee on Banking Supervision Guidelines, Corporate governance principles for banks, July 2015. Retrieved from http://www.bis.org/ bcbs/publ/d328.pdf.
3. Basel Committee on Banking Supervision Standards, (2014). Supervisory framework for measuring and controlling large exposures, Retrieved from http://www.bis.org/publ/bcbs283.pdf.
4. Chang, D. (1996). Applications of the extent analysis method on fuzzy AHP. European Journal of Operational Research, 95, 649–655.
5. Chernobai, A., A. Ozdagli and J. Wang. (2016). Business Complexity and Risk Management: Evidence from Operational Risk Events in U.S. Bank Holding Companies. Federal Reserve Bank of Boston Working Papers, No. 16-16.
6. Dombret, A. (2016). Digitalisation – Repercussions for banks and their supervisors. BIS, Central Bankers' Speeches.
7. Focarelli, D., D. Marquez-Ibanez, and A.F. Pozzolo. (2011). Are Universal Banks Better Underwriters? Evidence from the Last Days of the Glass-Steagall Act. ECB Working Paper 1287.
8. G-30 Group, 2012- "Toward Effective Governance of Financial Institutions", G-30 Group Reports, pp92.
9. Global Technology Audit Guide. (2012). Auditing IT Governance. Global Technology Audit Guide (GTAG®) 17. Retrieved from http://www.theiia.org/bookstore/downloads/freetomembers/0_1122_GTAG%2017.pdf.
10. Goetz.M, L. Laeven, and R. Levine, (2014), Does the Geographic Expansion of Bank Assets Reduce Risk? NBER Working Paper No. 20758.
11. ISACA -Information Systems Audit and Control Association- (2009) "The Risk IT Framework", Printed in the United States of America.
12. IT Governance Institute (2007), "IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance", Printed in the United States of America.
13. Khan, R. H. (2015). IT governance and IT strategy - Board's eye view. BIS, Central bankers' speeches. Retrieved from http://www.bis.org/review/r150806a.htm.
14. Lacković, I. D. (2013). Model for IT Governance Assessment in Banks Based on Integration of Control Functions. Management, Creating and Learning, Conference,2013.
15. Laeven L., L. Ratnovski, and H.Tong, (2014), Bank Size and Systemic Risk, IMF Staff Discussion Notes, SDN/14/04.
16. Lehman, J. A. (1985). Organizational size and information systems sophistication. Journal of Management Information Systems, 11(3), 78-86.
17. Moosa, I.A. (2006). Misconceptions about operational risk. J. Oper. Risk 2006, 1, 97–104.
18. Nastase, P. and S. F. Unchiasu, (2013), Implications of The Operational Risk Practices Applied in the Banking Sector on the Information Systems Area. Accounting and Management Information Systems, Vol.12, No.1, pp.101–117.
19. Prasanna G., A. Haldaney and S. Kapadiaz, (2011). Complexity, Concentration and Contagion. Journal of Monetary Economics.
20. Saaty, T. L. (1980). The Analytic Hierarchy Process, Planning, Priority Setting, Resource Allocation. McGraw-Hill, New York.
21. Sepahvand M. and S. Heidari, (2015). Using Interbank Payments Network to Assess Systemically Important Banks. Proceeding of the 4th International Seminar on eBanking and Payment Systems, MBRI. Sepahvand M. and M. Banitorof, (2014). Systemic Risk in Iranian Payment System. Proceeding of the 2nd International Seminar on eBanking and Payment Systems, MBRI.
22. Supervision and Regulation Letter, SR 15-7, Federal Reserve System. (April, 2015).Governance Structure of the Large Institution Supervision Coordinating Committee (LISCC) Supervisory Program.