Macrothink Institute™

Journal of Management Research
ISSN 1941-899X
2018, Vol. 10, No. 1

The Establishment of GRC Integrated Approach in Iranian bank's for Smoothing the Interaction with the International Banking System

Seyed Mehdi Hosseini

PHD of Economy

E-mail: Smhoseini@gmail.com

Sheida Asli

Master of Evolution Management

E-mail: Sheida.Asli@Yahoo.Com

Mohammad Rajabi

Master of Banking

E-mail: mohammad.rajabi@ Gmail.com

Sholeh Asli

Master of Banking

E-mail: Sholeh.Asli1@Gmail.Com

Received: Oct. 28, 2017 Accepted: Dec. 11, 2017 Published: January 1, 2018

doi:10.5296/jmr.v10i1.12172 URL: https://doi.org/10.5296/jmr.v10i1.12172

Abstract

In today's complex global business environment, having a clear vision of information and corporate governance approach, management and ensure the performance of compliance, risk and accepting it, are essential for the success of any organization. Organizations that choose corporate governance, risk management and compliance (GRC), at their forefront of their actions, have a competitive advantage. They well-informed their abilities in strategic

decision-making, and able to respond with agility and speed to the threats and opportunities that arise. Therefore, the concept of GRC, in recent years, has attracted the serious attention of banks and financial institutions at the international level. Banks, as financial intermediaries, play an important role in creating economic stability. Hence, the development of processes and structures in order to manage the activities of the organization, in line with the needs of beneficiaries, internal and international business regulations and requirements and business risks as well as ensuring the safety and health performance of these financial institutions are necessary and inevitable. In particular, in the current situation that the premises and the space necessary to interact with foreign banks have been developed, attention to the frameworks and international standards in the interaction between banks, including the implementation of corporate governance, risk management and compliance have the utmost importance. Hence, the concept of GRC at international level has attracted the serious attention that covers all the organization's activities in the three areas of governance, risk management and compliance. Implementation of GRC integrated approach ensures that an organization reaches its desired goals and vision if acts rationally. However, some challenges and structural constraints in the banking system of the country and the lack of comprehensive instructions, which is derived from the requirements and internal conditions of the country and is developed based on international standards, cause the importance of this issue will be trimmed in the banks and financial institutions.

Hence, in this study, first, the concept of GRC and the importance of its implementation in the banking system are explained and then, Different approaches to deployment GRC are included in the organization in and the following, we pointed to the relationship between GRC components, including corporate governance, risk management and compliance and examined the principles governing the establishment of each international authorities' perspective and challenges in the banking system in this context, presented suggestions in order to overcome obstacles and constraints in implementation of GRC, effectively.

Keywords: GRC, risk management, corporate governance, compliance, international banking

1. Introduction

Today, a pivotal role of the banking system in shaping economic processes is no secret. The banking system in each country has an effect on the economy, and makes achieving the macroeconomic objectives possible, and it is considered one of the major players in circulating the development wheel with controlling basic variables and for this reason, our country's banking system was targeted by sanction and has become one of the most vulnerable sectors of the economy in recent years.

Implementation of Barjam agreements in the past year and removing sanctions of banking system gave a valuable opportunity to the banking network so that after about a decade away from international intercourse, it provides conditions to enter forcefully into the realm of international banking, through compliance activities of the country's banks with standards, processes and coordination of global banking business. To connect with international banking, it is necessary to implement transparency in the framework of international standards.

As such, respecting laws and regulations and compliance with international standards are the interaction requirements and normalization of relations between the international bank and one of the concepts that has attracted serious attention in this regard is the establishment of GRC approach.

2. The definition of GRC integrated approach

GRC (Note 1) is a new concept, but it is a particular combination of overseeing concepts that have been raised in the past, with different methods in banks, financial institutions and other organizations, and it is such a way that converts an organization, from passive and discrete mode to dynamic and organizational mode.

"GRC is an integrated and encompassing approach that is defined in the establishment of corporate governance, risk management and respecting regulations across the organization and it is formed to ensure that the organization acts right according to the risk tolerance, policy within the organization and the external organization rules, in compliance with strategies, processes, technology and people" (Note 2). So important point in the establishment of GRC integrated approach is how to define and establish clear communication between the components of GRC and their responsibilities in the organization.

Changes resulting from the implementation of GRC, compared with the current situation can be stated as transforming from separate state to organizational state, creating a systematic approach, rather than a project approach, and coordination in processes.

An integrated approach to GRC should be taken. Organizations addressing each GRC area in a different way are likely to experience significant cost increases and duplication of effort. Taking a reactive, backward-looking approach to GRC could negatively affect efficiency and make the implementation of proactive, process-driven initiatives difficult, if not impossible. Good governance is about setting strategy, managing risk, delivering value and measuring performance.

A strong GRC framework ensures that the interests of stakeholders are adopted and implemented by management and staff members throughout the organization. Such a framework is the foundation of managerial integrity, making the best use of corporate assets and intellectual capital, and understanding and managing risk. All parts of a GRC framework are important components of good corporate governance.

2.1 The Three Elements of GRC integrated approach

GRC is a discipline that aims to synchronize information and activity across governance, risk management and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps. Although interpreted differently in various organizations, GRC typically encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations (Figure 1).Components of GRC integrated approach are as follows:

❖ Governance: is a set of activities that are conducted to execute strategy, proper implementation of policies and procedures, relation between policies, assessing policies in practice, assessing and updating policies and providing frameworks to observe regulations in an organization.

❖ Risk: includes set of activities that are required to identity and manage risks that are related to business and reducing the risk of not observing regulations through apt regulations.

❖ Compliance: refers to execution internal and external regulations and standards that are defined for the business. GRC results in covering policies and control, compulsory observance of regulations, accumulations of information that leads to business agility, establishing system to manage the businesstive advantage from extracted risks.

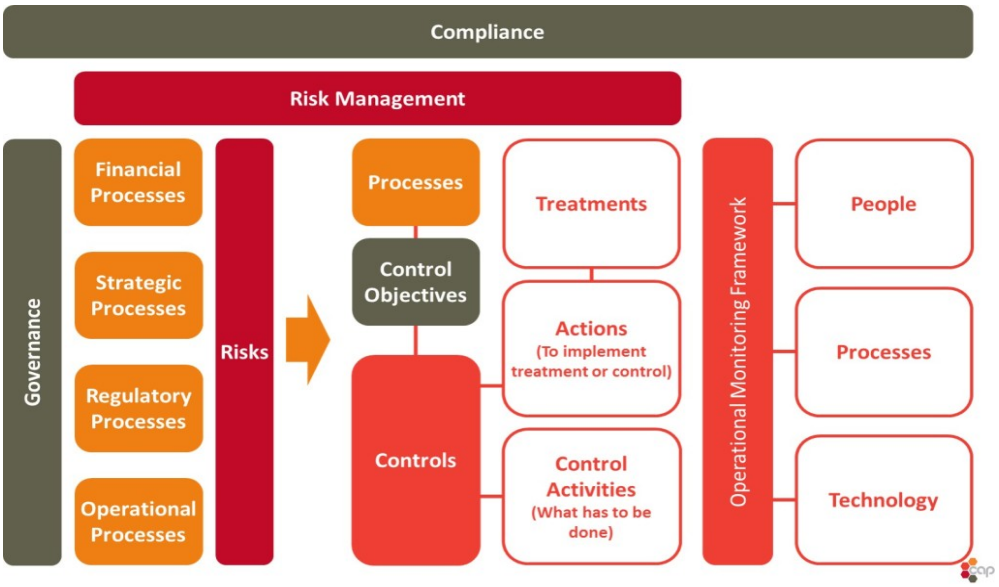


Figure 1. GRC elements and framework

2.2 Main Characteristics of GRC

The main Characteristics of GRC are as follow:

• Every employee and business are affected.

• Agreed strategy.

• Defined roles, responsibilities and authorities.

• Performance measurement and monitoring are centralized.

• Managerial responsibilities are decentralized.

• Process specific knowledge is required.

• Collaboration and cooperation between groups.

• High level of communication is required.

• Multiple and diverse systems and data sources.

• Ongoing change and refinemen.

2.3 Individual GRC Areas(market segmentation)

GRC program can be instituted to focus on any individual area within the enterprise, or a fully integrated GRC is able to work across all areas of the enterprise, using a single framework. A fully integrated GRC uses a single core set of control material, mapped to all of the primary governance factors being monitored. The use of a single framework also has the benefit of reducing the possibility of duplicated remedial actions.

When reviewed as individual GRC areas, the three most common individual headings are considered to be Financial GRC, IT GRC, and Legal GRC.

- **Financial GRC** relates to the activities that are intended to ensure the correct operation of all financial processes, as well as compliance with any finance-related mandates.

- **IT GRC** relates to the activities intended to ensure that the IT (Information Technology) organization supports the current and future needs of the business, and complies with all IT-related mandates.

- **Legal GRC** focuses on tying together all three components via an organization's legal department and chief compliance officer.

Analysts disagree on how these aspects of GRC are defined as market categories. the broad GRC market includes the following areas:

- Finance and audit GRC
- IT GRC management
- Enterprise risk management.

3. GRC Approaches

We have three different Approaches to integrate GRC**:**

1) Bottom Up

Line of business driven (complex, diverse and regional differences)

• Decentralized

• Little collaboration and coordination

• Overlaps and redundancies

• Interdependent process risks

• Costly

• Lack of transparency

2) Top Down

Centralized

1. Strategy

2. Resources

3. Operations

• Comprehensiveness

• Business Complexity

• Technology

• Collaboration

• Key personnel

3) Hybrid – Integrated Approach

Tone from the top

- Centralized strategy
- Decentralized resources and operations
- Highly collaborative
- Strong risk management
- Experis Finance
- Continuous Monitoring
- Transparency

Example of TOP-Down and Down- Top approach of GRC are given in follow figure:

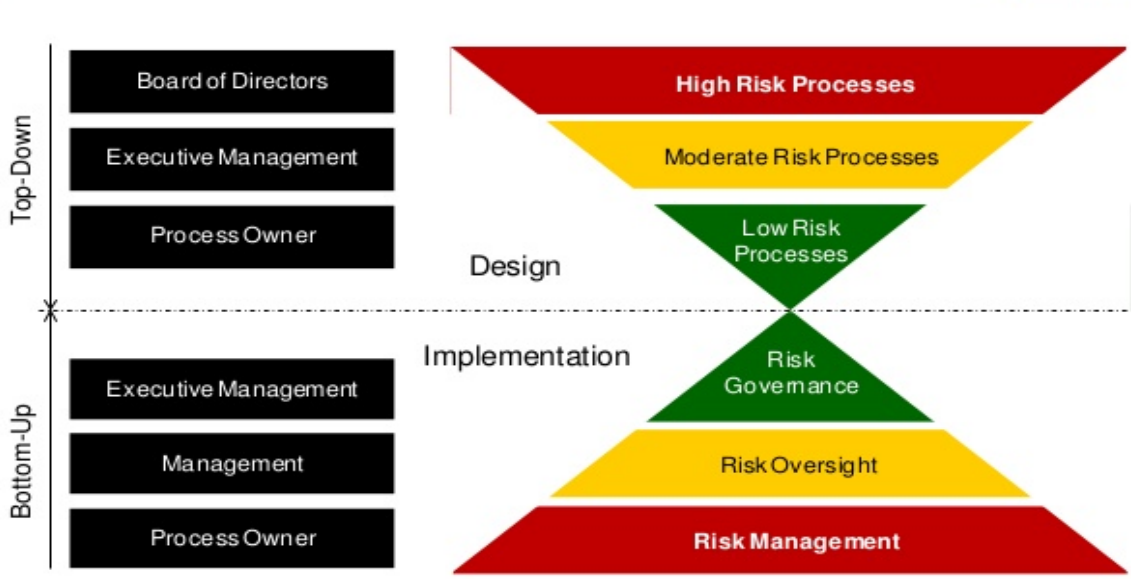


Figure 2. Example of TOP-Down and Down- Top approach

4. The value of GRC to all business

GRC promote the criteria unification, the effort coordination and collaboration between different characters involve in the direction of the organization through (Figure3):

1. The integration of the organs/government officials, administration and risk management, internal control and compliance

2. Role and responsibility assignation to key personnel
3. Communication channels formalization
4. Applying a risk-based approach
5. The implementation of a compliance program

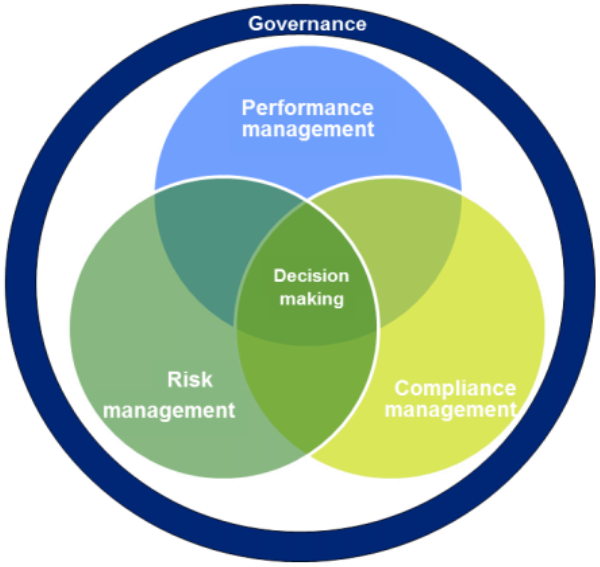


Figure 3. Role and responsibility of GRC

5. Reason and the deployment objectives of GRC approach in Banks

During the past few years, the global finance industry has seen an unprecedented surge in regulatory requirements, forcing a greater focus on the way organizations manage risk, especially financial risk. Regulators and credit rating agencies are demanding more transparency. At the same time, stakeholders and senior management are pressing for enhanced business value. Most firms have typically created fragmented and silo-based risk management and control programs. These siloed risk management programs are, however, not scalable; the technology supporting them is insufficient; and they do not merge into a common framework.

Recognizing the virtues of centralized GRC models, several forward-thinking institutions have already launched convergence efforts - integrating management of risk, compliance and control processes. The transition from traditional silo-focused systems to a holistic approach has plentiful benefits – streamlined risk and control programs; reduced input of time and resources; eased burden of corporate control units, such as internal auditors, compliance managers, and risk managers; and enabled multi-dimensional risk information for business intelligence. The endeavor, however, requires a well-communicated vision with clear roles and responsibilities. Need of the hour is a GRC solution that provides a clear, and unambiguous process for Governance, Risk and Compliance; and delivers a single point of reference for the organization to carry out these distinct yet entwined processes. Such solution is expected to synergize risk and compliance process leading to reduced cost and higher efficiency. Bank as a important financial company in Iran has to choosing one approach of GRC. Nowadays, we

have digital GRC which need subordinary to development. Deployment of GRC approach in banks leads to achieving the following objectives (Figure4):

-Formulation of controlling policies;

-Strict implementation of laws and regulations in the Bank;

-Increase the speed of business, through the focus of information systems;

-Create a system, in order to effectively manage the business;

-Determine the level of the bank's risk appetite;

Figure 4. Deployment of GRC approach in banks

5.1 The non-deployment challenges of the GRC approach in Banks

Banks and financial institutions nowadays seek more supervision solutions for their IT systems so it seems necessary to use GRC measure. GRC is not a new concept rather it is a specific combination of supervision terms which were used previously by banks, financial institutions and other organizations in various forms. These systems are not merely an approach to conduct business rules rather they are solutions to integrate regulations with organizational structure as well as alignment with daily business processes It has to be noted that GRC is not separate from ERP and is implemented on ERPs

Many organizations manage the activities relating to corporate governance, risk management and their compliance, individually (so-called in silo) and in the form of various projects with multiple applications, so that, the administrative process of each sector will be designed based on separate requirements and guidelines, regardless of their relationship and dependencies for each other.

Our GRC approach focuses on maintaining the right balance between risk and reward. An effective risk management program focuses simultaneously on value protection and value creation.

The result of this approach faces the organization with the following challenge:

-Incompatibility between different projects;

-Lack of unified attitude between risk and compliance and subsequently, limitation in the decision-making process;

-Lack of scalability (Note 3) from the organizational perspective;

-Doing repetitive activities that increase the costs;

5.2 The benefits of the GRC approach for Banks

While, the organizations intend to use software solutions, in order to enable processing of each GRC component, because of lack of attention to the relationship between the components, they confuse and suffer a lot of time and cost, for managing each of these processes. This is the case that adapting the GRC approach requires the integration and development of a single system for managing GRC approach areas, and can have the following benefits for the organization such as banks:

❖ **Cutting costs** –The integrated approach of GRC often brings real financial benefits as unnecessary spending can be cut, while the clearer focus can help boost revenue at the same time. The bigger the business, the more likely it is that there will be plenty of areas where there is crossover and wastage, so a process like this can transform efficiency.

❖ **Less duplicated work** – This is where most of the cost-cutting can be made, but it's about more than just the money. Having similar processes duplicated across a business is a hugely inefficient way to operate and GRC can free up whole teams to work on other projects.

❖ **Less negative impact** – Having too many procedures, especially ones that aren't working in a logical manner, can waste a lot of time for staff across a business. Tying everything together in an GRC strategy cuts down on the paperwork and bureaucracy, which will boost your staff's productivity, not to mention their morale.

❖ **Greater information quality** – A more centralized and consistent approach to governance, risk management and compliance helps to not only speed up the processes for gathering the necessary information, but also improve the quality of what is gathered, helping decisions be made more rapidly and with greater confidence.

❖ **More ability to repeat processes** – Another huge benefit is that processes can be standardised across these areas, allowing for them to be repeated more easily and with greater consistency and efficiency.

❖ **Reputation security** – Risk management and compliance are both essential parts of any attempts to secure your business's reputation, so it goes without saying that managing these aspects more efficiently provides a more effective method of reputation security.

❖ **Better allocation of resources** – Getting more information and understanding more about areas that are duplicating work can help determine the most effective directions for your business to go in.

❖ **No more silos** – Any large business has numerous issues with staff working in 'silos' where information doesn't flow in or out in a productive manner. GRC won't completely eradicate these issues, but it will certainly minimise their potential impact on key areas.

5.3 Describing the relationship between the components of GRC

The following illustration shows the components of GRC (Figure 5). This model shows a close relationship between corporate governance and risk management and compliance, in which with appropriate and robust standards for corporate governance, we can improve the risk management process and by integrating risk management and internal systems, we can trust the development of corporate governance high standards. In the GRC approach, risks management and compliance will be integrated with each other, and then the corporate governance will be applied to them, as an umbrella.

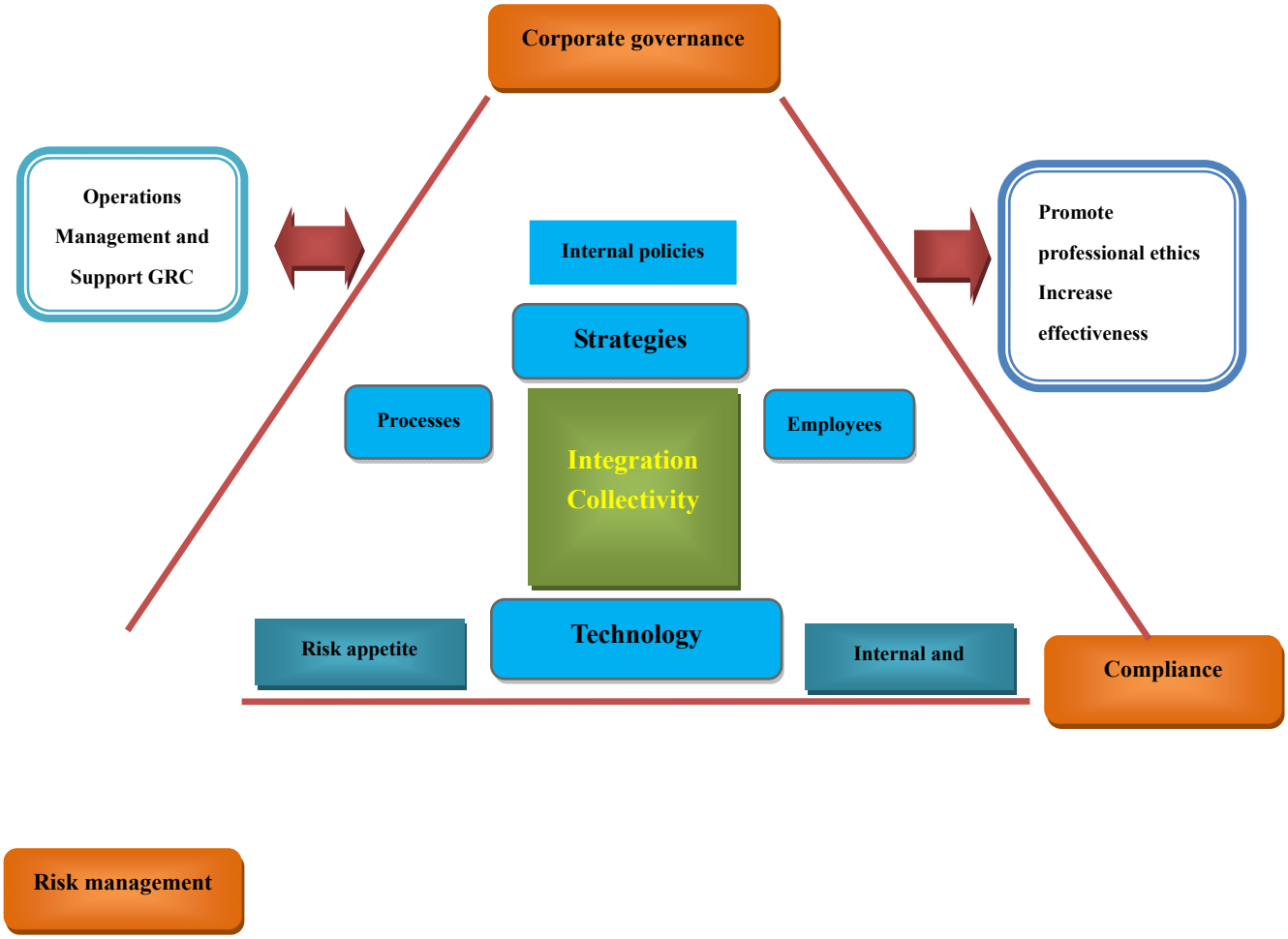


Figure 5. The relationship between the components of GRC

Thus, corporate governance is considered a key component of GRC, and corporate governance mechanisms, such as risks and audit committees and the use of internal and independent auditors leads to accurate and transparent reporting of financial events, access of the stockholders to the important financial information and performance monitoring of Banks' executive management. Therefore, in the following, we refer to the relationship between each component, and explain the GRC components (Figure 6).

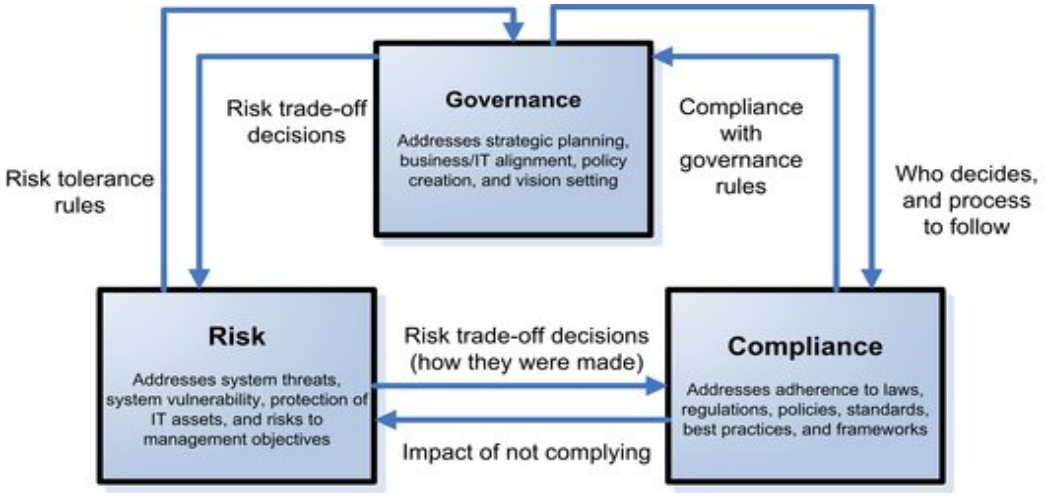


Figure 6. Activities and responsibilitiy of risk, governance and compliance in GRC

In this Figure we have three separate sets of processes—governance, risk, and compliance—any of which can take place simultaneously or in tandem with the other processes. For ease of understanding, however, this will discuss these interconnected activities as separate processes:

- Establish IT governance.
- Assess, monitor, and control risk.

5.4 GRC approach implementation phases

1) Analysis of the organization's current situation in the field of GRC

Prior to the implementation of GRC approach, the current situation of the organization should be examined, in terms of infrastructure, processes, facilities and etc.

2) GRC Modeling

This phase includes activities such as, the definition of a common language between components, the development often appropriate organizational structure; determine the relationship between types of risk, control and integration of process.

3) Operation of GRC

This includes activities such as, documenting processes, risk and control audit, reporting, reforming programs and storage of information.

4) GRC automation

In order to avoid conducting parallel activities and reduce costs, following GRC operation modeling, component processes will be done integrate and online and in the form of GRC automation. In this phase, activities will be done such as, control testing, determine the key performance indicators (KPI, KRI) (Note 4) and identify anomalies BCP (Note 5)

The Maturity Model for Integrated GRC focuses on building the five levels of capability outlined below over time and implementing the broad strategy as a series of tactical intelligently designed actions**:**

- **Siloed**

The Siloed stage focuses on baseline activities needed to manage risk and is the starting point for all organizations. At this stage the organization is not necessarily deficient in its approach but coordination across functions is very limited.

- **Managed**

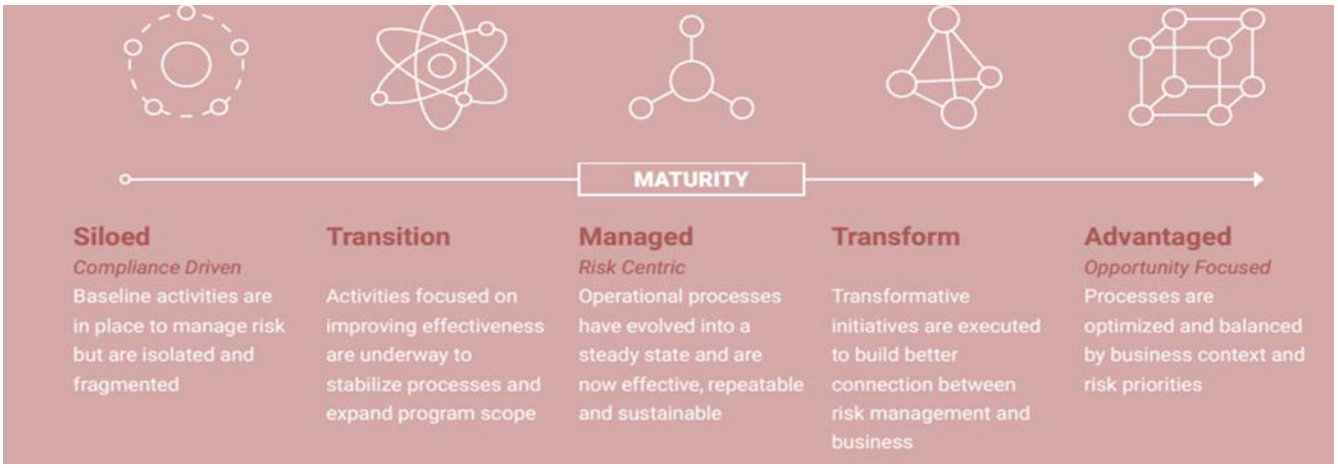
The Managed stage depicts the phase at which organizations reach a coordinated, sustainable program. The GRC program, at this point, is effective and achieving its objectives but is still lacking the critical connection to the business that will turn the effort into a valuable contributor to the business strategy.

- **Transition & Transform**

The Transition stage and Transform stage help the organization"move to the next level" with initiatives that evolve critical capabilities and set the stage for advanced capabilities.

- **Advantaged**

The Advantaged stage is designed to be achievable for most organizations. This is not an 'ideal, pie-in-the sky' aspiration but an advanced stage of maturity that optimizes the GRC program. At this point, risk and compliance is part of business operations and the organization reaps the benefits of a coordinated program.



5.5. Important principles in the implementation of GRC approach

1) Identifying important challenges: with regard to the fact that the establishment of GRC approach is faced with multiple challenges and sometimes, unpredictable and overcoming all

challenges at the same time is not possible, therefore, it is essential, first, the challenges are prioritized and based on that, eliminate the challenges.

2) The establishment of a joint working team: a joint operational committee should be created in order to the success of GRC approach, which its sole responsibility is to deal with issues related to GRC. This cause all the issues will be discussed in a single structural form and solutions will be developed in the ways of cooperation.

3) Assigning tasks in the least amount of time: the effectiveness of GRC is originating from the fact, that the information in all business lines is shared. Also, tasks and responsibilities related to GRC need to be clearly defined and management should also ensure that no task is repetitive and parallel.

4) Avoid builds another silo: GRC is an approach that aims to implement and it is supported from compliance management, and risk management, which are previously existed. Therefore, its implementation should not lead to the creation of new silos and additional structures.

5) Ensure the possibility of implementing the processes, before investing in new technologies: However, new technological tools are designed and presented to support GRC, however, before investing in a new technology related to the field, ensuring the GRC requirements and the ability to support current systems from the new system is essential in order to meet the needs of today and the future of business organizations.

6) Creating an effective environment: an understanding of the functional role and responsibilities in this field can have a significant effect on detecting and removing duplicate roles, and, in addition to avoiding any incompatibility, it leads to the optimal allocation of resources and saving costs.

7) Establish a common understanding of risk: by adopting a common methodology and approach to identify and assess the risks of an organization, one can create a structure that provides a broader view of all the associated risks over the activities of the organization and it will be possible to analyze data with high flexibility.

5.6 Business approach for GRC in Iranian Banks

Here are common definitions of the three different business approaches and architectures to GRC:

- **Decentralized:** This is the most immature approach to GRC, even referred to as"anarchy" by Rasmussen. Under a decentralized scenario, risk management and regulatory compliance activities are performed in multiple silos throughout the organization. Responsibilities are scattered, which leads to a situation where there are big differences between departments. This approach is also usually characterized by manual GRC activities (e.g. emails, document, spreadsheets, etc.)

- **Federated:** Under a federated GRC approach, there are common taxonomies, standards and methods for risk identification, management and reporting throughout the enterprise. However, distinct risk methods, taxonomies and workflows are also supported, in order to meet

unique needs across the company. A federated GRC architecture is characterized by central coordination and shared services with distributed accountability and autonomy where it makes practical sense. There is GRC oversight at the corporate level but the actual management of GRC is performed more at the department level. Risk functions from different departments work and collaborate together.

- **Centralized:** This approach to GRC has some things in common with the federated GRC architecture, namely the presence of common taxonomies, standards and methods for risk identification, management and reporting. However, under this GRC architecture and strategy, GRC efforts, processes, and services are coordinated at the corporate level across the entire company, with less autonomy at the department level. There is a common GRC platform, but more importantly, there is centralized GRC coordination.

If we are going to choose any of these three approach, we can easily disqualify the decentralized approach. Because of the need to manage Risk holistically (EHS and Sustainability also for that matter), with an alignment of standards, methods, objectives and reporting across the enterprise, the decentralized GRC architecture does not make sense.

Before going explain suggested approach, explain each of components document of Iranian Banks according to discipline and legals:

5.6.1 Corporate Governance

Corporate governance involves all the processes and structures, which helps financial institutions, in directing and leading affairs with the aim to ensure its safety and security, coupled with an enhancing return on equity. According to the OECD definition of the corporate governance," corporate governance is the set of relationships between management, board, shareholders and other interested parties in a company".

With the establishment of corporate governance in the organization, correct division of tasks and responsibilities between shareholders, board of directors and executive managers, leads to ensure the performance of the managers by shareholders. In contrast, poor corporate governance can lead to financial instability and as a result, it increases the risk of companies and financial institutions.

5.6.1.1 Principles of Corporate Governance

One of the last published principles, globally, on corporate governance was released in 2004 by the Organization for Economic Cooperation and Development, which is presented in six areas, as below:

Principle 1. Provide the basis for an effective corporate governance framework;

The corporate governance framework should be transparent and increase market efficiency, compliance with the rules and regulations, and divide responsibility, clearly between the various regulatory, legislative and executive authorities.

Principle2. The rights of shareholders and key ownership functions;

The corporate governance framework should support the shareholders' rights, and facilitate this important matter.

Principle 3. The equal conduct with shareholders;

The corporate governance framework should assure a fair conduct for all shareholders, including minority shareholders and foreign shareholders.

Principle 4. The role of stakeholders in corporate governance;

The corporate governance framework should recognize the rights of all stakeholders, based on law or bilateral agreements and provide more cooperation between companies and stakeholders.

Principle 5. The disclosure and transparency;

The corporate governance framework should assure an accurate and timely disclosure for important issues about the company, including financial situation, performance, ownership and corporate governance.

Principle 6. Responsibilities of the Board of Directors, including internal control, internal audit, etc.;

The corporate governance framework should assure the corporate guidance with long-term vision, effective monitoring of management by the board of directors and board accountability to the company and shareholders.

5.6.1.2. The importance of corporate governance in the banking system

Corporate governance is one of the important issues in the field of finance that plays a significant role in improving the performance of financial institutions, including banks and facilitates access to health and stability of the financial system. In fact, the corporate governance system is a monitoring tool that provides the context, to increase transparency and efficiency, reduce corruption, respect for the rights of all stakeholders and accountability of the management system. On the other hand, weakness and inadequate attention to establishing proper corporate governance at the bank reduces their ability to detect, monitor and manage the volatile risks. Hence, in international transactions, corporate governance issues have special and significance importance, due to the specific characteristics of banks, and it shows the importance of their implementation in the financial institutions, compared with other institutions. Among these characteristics, we can point to the following matters:

-Being a risk taker bank;

-Institutions with high financial leverage;

-Asymmetric information on banks;

-Responsibility to protect customers' deposits;

-Stabilizing factor in the country's economy;

-Transferability of crisis from one bank to other banks;

5.6.1.3 The objectives of establishing corporate governance in banks

In terms of banking operations, corporate governance is a way in which, the Board of Directors and executive management monitor working issues and relationship through it to achieve the following objectives in the organization:

• Achieve economic returns for shareholders;

• Correct implementation of the organization's daily operations;

• Identify the interests of stakeholders;

• Verification of the operations of the Bank, in accordance with governing laws and regulations;

• Protect the interests of depositors.

5.6.1.4 Requirements of establishing corporate governance, in terms of international bodies

1) Basel Banking Supervision Committee

From the perspective of the banking industry in Basel Banking Supervision committee, corporate governance is the distribution of powers and duties of the Board of Directors and Executive Board and the practices of administering the activities and affairs of a bank, by them. This method includes the following tasks:

-Determine the strategy and goals of the Bank,

-Determine tolerance strategy / risk propensity of banks,

-Perform daily activities of the Bank,

-Protect the interests of depositors and bank obligations, in return for the shareholders and considering the interests of other stakeholder groups that have been recognized,

-Aligning activities and management working practices, in accordance with the laws and regulations in force.

2) Organization for Economic Cooperation and Development

From the perspective of the OECD, corporate governance is" a set of relationships between management, board of directors, shareholders and other stakeholders of each company." Also, it determines the structure, by which the company's objectives and instruments to achieve these objectives and monitoring their performance are determined. Good corporate governance should provide appropriate incentives for the Board of Directors and Executive Board to follow the organization's objectives and in line with the interests of the company and its shareholders and facilitate effective monitoring. The existence of an effective corporate governance system in each company or group of firms, or more generally, in the economy, helps the necessary confidence for correct operation of the economy, based on the market.

3) Islamic Financial Services Board

Islamic Financial Services Board has recommendations for applying the principles of corporate governance for institutions offering Islamic financial services, which has two principles: the first principle announces that institutions offering Islamic financial services should create a comprehensive corporate governance framework, in which roles and strategic tasks of each corporate governance section will be appeared and balance mechanisms for responding to the various stakeholders will be created. The second principle is stated that in the appointment of members of the corporate governance committee, the Board of Directors should ensure that each member will have an important role in the committee.

5.6.1.6 Study tools of corporate governance in the banking

For the implementation of corporate governance in the banking system, the use of internal control means, risk management and compliance is essential. Internal controls are set ofpolicies, approaches and procedures, which are adopted by the board of directors and senior managers in an organization to achieve increased efficiency and effectiveness, reliability of financial reporting and respectingthe laws and regulations. Also, banks should have a system to manage their risks, which helps them in the identification, measurement, monitoring and proper control and, ultimately, effective risk management. Creating compliance units are mandatory to ensure the compliance of rules and regulations with internal and international standards. Then, each of the tools mentioned above are described in detail.

❖ **Internal control system**

An efficient internal control system is essential for the safety and security of all financial institutions. Such a system can guarantee recognizing objectives of the institute and increase the long-term profitability. Internal control is essential to ensure the monitor, manage and promote a healthy culture in the institution. The internal control system should be organized based on a range of qualitative principles, such as”organizing, self-control, continuity, inclusiveness, independence, informative, coordination, quality of employees", in order to achieve its goals. Therefore, internal control is a continuous process that the board members, senior managers and working staff should participate in it at all levels of the bank, and its aim is to ensure banks achieve the objectives. Internal control is not the only implemented policies and a procedure at specific time points, but it is a continuous operational measure at all levels of the bank.

The internal control system should be continuously monitored, to ensure its compliance with the regulations and procedures, limitations of risk, revision, regulations and authorities. Without an effective channel of communication and the rapid and timely access to important information regarding all activities of the bank index and external market conditions, which are associated with decision-making, the successful implementation of a control system will not be possible. Internal auditing system, which is an important part of internal control, must be strong and independent and its report should be sent directly to the Board of Directors and senior management.

❖ **The establishment objectives of internal control**

The main establishment objectives of the internal control process in banks are as follows:

-Efficiency and effectiveness of activities;

-Reliability, completeness and timeliness of financial information and management;

-Respecting applicable laws and regulations;

The first objective is a functional purpose, which refers to efficiency and effectiveness in the use of assets and other resources, and as a result, to protect the bank against losses.

The second objective is an information objective, which relates to timely prepare, reliability and relevance of case reports needed for decision-making in the bank. Also, it refers to the needs of shareholders, the board, observers and other organizational external parts (those that quality and completeness of the information is a necessity in their decision-making), the financial statements, annual accounts, reliable, and other financial information.

The third objective is a compliance objective, which must be achieved to ensure the reputation of the bank, and this is possible by paying attention to laws and regulations, regulatory requirements and organizational policies and procedures.

5.6.2 Risk Management

Although financial innovations and initiatives in recent years in the fiscal and monetary areas at the international level, stimulated and facilitated work-business and business of firms and economic actors, however, given the intricacies of these inventions, including securities and derivatives, they increased the risks of banks and financial institutions, and followed by volatility in financial markets. The financial crisis of 2008 can be outlined, in this regard that its origin was mortgage loans for housing in the US market.

The effect of risky behavior in banks and financial and credit institutions in the formation of the financial crisis and its effect on other international financial and economic markets in recent decades led to increase the sensitivity of regulatory bodies about the accurate performance of banks and reliability of the management and control of risks associated with their activity, more than ever, and with laws and regulations, forced banks to do self-control and monitoring measures and manage risks. Central Bank of Iran, as the supervisory authority of the country's banking system, and according to the importance and necessity of having the right system, for effective management of risks, has developed and delivered a series of guidance (based on a statement by the Basel Committee), to effectively manage the bank risks. Therefore, it is necessary for the banks to provide the effective implementation of these directives and regulations by creating appropriate organizational context and providing the necessary mechanisms.

5.6.2.1 The need to implement risk management

The most important reasons for implementing risk management in banks are as the following:

1. Globalization and deregulation of banking services;

2. Intensification of competition in the local and global markets;

3. Increased corporate bankruptcy process and the need to predict the possible bankruptcy of firms, while receiving credit;

4. The development of financial markets and increase innovation in monetary and financial instruments;

5. Increase and diversify risk factors in banks and credit institutions, because of the complicated equations and economic relations;

5.6.2.2 Requirements for risk management in the banking industry, from an international perspective

Given the extent of the risk, important risk management, such as credit risks, liquidity, operational market, is in the priority. In accordance with the provisions of the Basel Committee, banks and financial institutions are required to identify, assess, monitor and control all important risks and overall assessment of capital adequacy and on this basis, any bank should have a comprehensive process of risk management, fit with its size, volume and complexity of organization. The importance of this issue will be deeper, when the Basel committee develops rules (2), in a short time, after the implementation of the Basel provisions (1), and it was mentioned, the banks that do not implement Risk Management Plan, will be limited in their financial and money transactions, with international banks. It has also been emphasized in the guidelines issued by the Basel Committee, and sending directives of the Central Bank of Iran, including "Instruction guidelines for an effective system of internal control in credit institutions". Also, the provisions of Basel 3 are now applied in America and Europe, and according to a schedule, by the end of 2018 all its branches must be fully implemented.

5.6.2.3 Executive structure of risk management in banks

Executive structure of risk management includes different organizational levels, such as the Board of Directors, Risk Management Committee, the Executive Branch of risk management and risk assessment subcommittees.

- Risk Management Committee: it is a specialized Committeethat acts to facilitate the realization of supervisory responsibilities of the board, in the area of risk management in order to effectively monitor the analysis, control and determination of Banks' risks and has the responsibility for developing strategies and risk management policies. The main purpose of the formation of the Risk Management Committee is assisting the Board of Directors of the credit institution to monitor the following:

• Determine the status of credit institution's risks;

• Performance evaluation of systems used to determine the risk limits;

• Control credit institution's risks;

• Analysis of risk;

• Review and approve major transactions;

-Subcommittees of risk assessment: There are independent Committees to control, evaluate, eliminate or reduce risks and identify obstacles in the way of implementation and also to correct the processes related to risk management.

- Executive Risk Management Unit: This unitacts in the bank as a trustee to track major risk management (credit, liquidity, market, operational).

5.6.2.4 The consequences of non-implementation of risk management, in banks

The consequences of the lack of risk management, in banks are as follows:

-Lack of attention to the required capital adequacy in the bank, according to assets and high-risk activities;

-Proper evaluation impossibility of the quality of assets and Bank's debt;

-Notable gaps in liquidity and its problems;

-Lack of accurate estimation of resources, costs, revenues and expenditures;

-Unforeseen costs, such as payments of outstanding claims;

-Lack of competition with the banks that have appropriate risk management;

-Inability to estimate cash caused by hazards ahead and disability in adapting necessary preparations to reduce or neutralize them;

-Information deviation of managers, which resulted in non- optimal, decisions;

-Reduced profitability, due to lack of identification and collection of income;

5.6.3 Compliance

According to the concept, "compliance" includes the processes and controls, which leads to a certain respect of the rules, regulations and procedures and in the banking system, it means" the consistency of credit institution activities with the laws, regulations and standards associated with its activities," which its violation or ignorance leads to compliance risk.

5.6.3.1 The requirements of the Central Bank of Iran, in line with the implementation of compliance, in banks

Create the compliance section was done for the first time, in accordance with the provisions of the basic principles draft of setting compliance monitoring by the Committee on Banking Supervision, Bank for International Settlements (Basel), with aims to regulate risk management, the creation of an independent part of the banking activities in the bank, as part of compliance. Accordingly, the necessity to establish the evaluation and compliance unit, in accordance with Article 39 the regulatory policy of the banking system was notified and stressed in 2008 from the Central Bank to banks that any foreign exchange obligations, Rial contracts and obligations, warranties and any kind of obligation should be done after review and approval of this unit, in terms of compliance with domestic and international legal and banking laws and regulations. The article mentioned in paragraph 32, regulatory policy was

reaffirmed in 2009and for a six-month period was considered for it. Then, the country's banks were asked to announce the measures done in relation to the establishment of evaluation and compliance unit to the central bank.

5.6.3.2 The objectives of the compliance unit in banks

The purpose of compliance unit is assisting banks in compliance risk management. As such, compliance unit should try to ensure the compliance of the bank's performance with domestic and international laws and regulations, and support the interests of the banks and stakeholders with reducing compliance risk. Therefore, the following objectives can be considered for the compliance unit:

- Compliance with the laws, regulations and standards as well as the Central Bank of Iran notifications;

- Recommending appropriate corrective actions in detecting violations of banking laws;

- Avoiding any significant harm, damage to the reputation of the institution and fines, legal penalties or regulatory punitive;

Remarkably, according to the laws, regulations and standards in the field of business, financial services can be offered at two levels:

Level 1.Compliance with internal laws, regulations and standards

Level 2. Compliance with international laws, regulations and standards

Finally, preparing a measurement dashboard of GRC is concerned, that can provide the necessary information. In the figure below, you can see the international binding requirements and regulations, and scoring components for the establishment of GRC.

6. Challenges of the banking system in the implementation of GRC

There are limitations for the establishment of the GRC in the banking system, which prevent from reaching a part of the objectives. In the following, some of these limitations are pointed out in the separation of different areas of GRC (Figure 7).

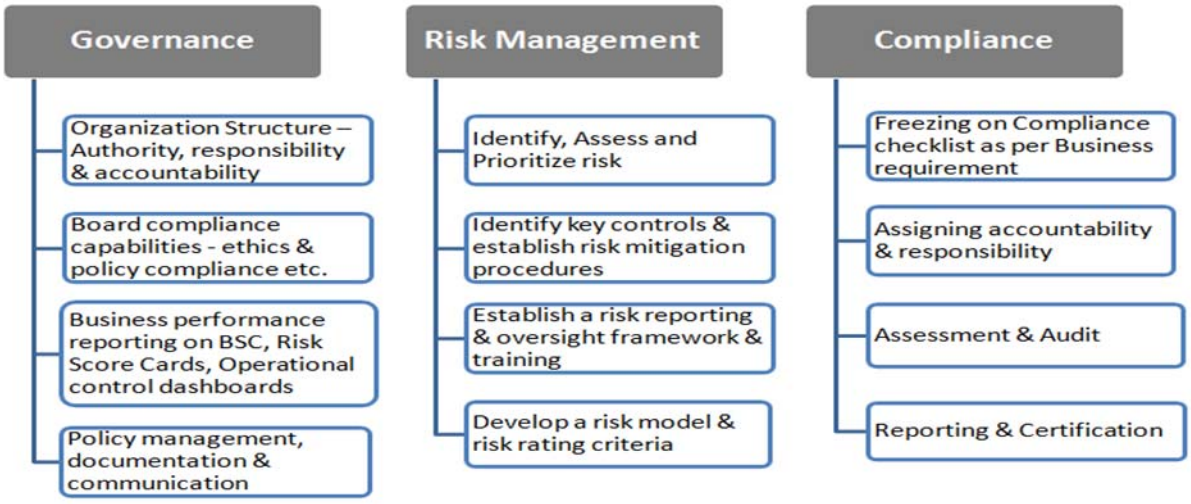


Figure 7. Measurement and scoring policies to GRC

6.1 The establishment of corporate governance challenges in banks

❖ **The way of choosing a managing director in the public banks**: Based on the principles of corporate governance, managing director of the bank should respond the board members about the implementation of the board's decisions. However, based on existing conditions, because of the delegated powers from the Managing Director of the bank to the board members, they have to respond their performance to the Managing Director of the Bank. This can be investigated, as a limitation in the implementation of corporate governance in the public banks. It should be noted that, the central bank has tried to remove barriers of the corporate governance implementation in the banking system of the country and the implementation of the supervisory duties separation principle of the executive duties of the board of directors of the banks, and it has approved a ban on holding the post of managing director and chairman of the Board of Directors by one person at the same time in the new founded private-public banks and non-bank credit institutions. However, in some banks, still, the post of CEO and chairman of the board of directors at the same is not limited.

❖ **Lack of transparency in financial statements of banks:** Central Bank of Islamic Republic of Iran has notified an Act, entitled, "regulations on minimum standards for transparency and public dissemination of information by credit institutions" to the country's banking system, in order to provide areas of corporate governance implementation in the banking system. Based on the above-mentioned Act, banks are required to disclose indicators and their management for a variety of liquidity, credit and operational risks, in their financial statements. Implementation of the above Act could lead to increased recognition of customers from the banks, in terms of safety and efficacy, and cause their informed choice. Despite the benefits listed by the Act mentioned, some banks, especially state-owned banks are excluded the implementation of the Act because of limitations, which makes the transparency of financial statements difficult in the banking system.

❖ **Difference in providing the stakeholders' interests:** The interests of stakeholders are the other cases that limit the implementation of corporate governance in the banking system of Iran. In conventional banking, stakeholders' interests will be provided by setting interest rates before, whereas, in the Islamic banking system, applying this approach is contrary to Islamic law. Therefore, a new model is required to be based on Sharia law and the country's monetary and banking in the Iranian banking system, in order to protect the interests of stakeholders, particularly depositors, so that, it will be in accordance with Islamic Sharia law.

❖ **The absence of an operational audit to assess the performance of managers and Accounting Standards for the risk:** in order to achieve transparency, the most reliable report is the auditor's report and the legal inspector, with the financial statements, which, despite pointing to non-compliance with accounting standards and directives, they have not sufficient operational capabilities and do not require the banking system to modify the performance, even due to the responding duty requirements. This reflects the legal and structural problems and shortcomings in the country's monetary system, and the necessary reforms should be done in this regard.

❖ **Non- localization laws and international regulations, according to the terms and the country's banking system:** according to the need to implement corporate governance in the banking system and inconsistent patterns in traditional banking system with the banking system without usury, it is necessary to design and develop a model appropriate to the situation and the needs of the banking system, to implement corporate governance from the central bank of Iran. However, the central bank has translated and published documents, titled "Strategies for localization of effective corporate governance in the banking system of Iran"," Improving corporate governance in the banking units" and" principles guidelines of corporate governance for institutions offering Islamic financial services", in order to provide context for the implementation of this important action, however, the reports have been merely a translation of the patterns in other countries, and in fact, so far, no localize and comprehensive pattern have been presented from the central bank, in this regard.

6.2 Challenges for the implementation of risk management in banks

❖ **Weakness of infrastructures and lack of comprehensive in customers' information banks:** Implementation and establishment of risk management in banks require infrastructure and creation necessary foundation, such as developing a comprehensive customer information bank and access to clear and accurate data in all the sectors.

❖ **Lack of banks' uniformity in the establishment of risk management:** lack of laws and notified regulations transparency by the supervisory authority, regarding the establishment of risk management, resulted in each banks act in personalization and mainly, based on internal policies and tailored to their needs in different risk, and do not follow a fixed pattern in risk management.

❖ **Lack of skilled manpower in the field of risk:** risk management process is a dynamic process and each bank is exposed to diverse and variable risks according to their activities. Therefore, the condition of banks' success is in effective risk management, ability and

capability of risk in the face of all risk types, and their management, that it depends on the ability of managers and experts in the risk section on the face with these conditions. Currently, a major part of the country's banking system lacks skilled manpower in the field of risk and therefore, experts active in this sector should directly benefit from educational, specialized and practical courses of risk management inside and outside the country, to achieve this important matter.

❖ **Limitation in the use of foreign applications and the inadequacy of software produced by domestic enterprises in the field of risk management:** a number of barriers in the use of risk management foreign applications, including incompatibility or supporting problems of the purchased software by foreign companies, due to the specific conditions of the country (sanctions), have caused limitations for the country's banks to purchase the software. Notwithstanding that the software produced by domestic companies in the areas of risk is not localized for real and are not able to meet the needs and demands of the banks.

6.3 Implementation challenges of compliance in the banks

-Lack of adequate technical knowledge in the areas of compliance management in the country: According to the new issue of compliance the country's banking literature, and the lack of sufficient technical knowledge in this field, in practice, banks are faced with some limitations and problems in the creation of these units and in the development of processes and defining the tasks.

-Lack of skilled human resources in the field of compliance: training bank employees in terms of required expertise in the compliance section play an implement role in the implementation of corporate governance. Unfortunately, the lack of skilled manpower in the country and limiting conditions for specialized training of bank employees, abroad, in practice, has created a lot of constraints in the implementation of compliance section.

- **The weakness of domestic companies in producing the software needed to implement compliance:** problems arising from the implementation and use of foreign software, due to a lack or deficiency of infrastructure and existing data as well as the lack of proper support from the software by foreign firms for various reasons, such as banking sanctions, in recent years, caused the banks turn to domestic companies, however, domestic produced software do not have the necessary integrity to cover the needs of banks.

-Inadequacy of the notified executive regulations and directives of supervisory bodies in this area: in spite of, publication of guidelines on the establishment issue of the compliance section in banks, on behalf of the Central Bank of Iran, its implementation has been neglected in the banks, for reasons such as lack of transparency of regulations and insufficient executive guidance as well as no administrative records.

7. Conclusions and recommendations

Implementing an Integrated GRC program is not a simple task. Most organizations build siloedunctional programs first. To date, only those organizations that realize Integrated GRC is an opportunity to transform risk into a competitive advantage, or ones that have suffered

substantial negative impact from realized risks or compliance enforcement, have aggressively sought to mature their GRC programs. Now, however, the velocity of growth in compliance requirements and exponential expansion of risk affects every company. The need for Integrated GRC has never been greater.

Companies in the Siloed stage must ensure their individual functions are responding to risk and compliance drivers effectively first. Before any integrated activities can take place, at a minimum, key functions need to understand their role in managing risk and meeting compliance requirements. In order to move from Siloed to Managed stages, organizations Transition through projects that catalog and organize GRC efforts and build the business case to take GRC to the next level. Companies in the Managed stage see much better visibility into risk and compliance issues through communication between executive stakeholders and GRC executors, common taxonomies for the basic elements of GRC and an integrated technology strategy. In order to reach the Advantaged stage, GRC processes Transform through more rigor and a regular cadence of governance activities, taxonomy implementations and monitoring metrics to identify where the program is working effectively and where gaps still need to be addressed. This allows the organization to harmonize GRC efforts across business requirements and reduce administrative overhead and costs. Organizations in the Advantaged stage are ready to realize the competitive advantage of harnessing risk such as beating competitors to market, launching new products and services with calculated efficiencies and avoiding major issues that affect reputation and the bottom line. Organizations in this final phase speak risk in the “business' language” and are able to identify and respond to emerging business requirements ahead of the curve using a well-oiled integrated GRC program.

So, According to challenge of GRC in Iran as a system, Maybe in Iranian banks the Federated Approach is the Best. In this approach, different groups within the organization share services, technology and information that can be used in different ways. Organizations can “harmonize and rationalize” their enterprise and local business units levels under this approach. Organizations in all industries have matured their perspectives on GRC and are expanding their initiatives to cover an integrated and enterprise-level view of risk and compliance. The goal is to effectively define, manage and monitor the external and internal business environments to assure the protection and growth of value within risk tolerance and legal boundaries. This involves moving toward a federated organizational structure, where GRC functions are centrally overseen, but responsibility is distributed across all lines of business. that organizations might still have visible compliance leaders that organize and ensure everybody is working together. However, what is most important is that the organization created a compliance architecture. This architecture creates a framework where all the different compliance roles can come together for strategic planning and information sharing.

To pull this off, organizations need technology that enables this framework because organizations are often buried in documents such as e-mails and spreadsheets that are difficult to produce and share. This allows organizations to become intelligent in managing compliance issues across many departments sharing the same architecture. But Iranian banks have a lot of problems.

As mentioned, the GRC approach in banks has been proposed as a new approach that its establishment requires a common language, building a single database, information and documentation attachment (Note 6), design and implementation of a standard work procedures and creation of a communication channel, among all the activities of banks. The objective of establishing GRC approach can be considered in the formulation of controlling policies, requiring the implementation of regulations on bank level, accelerating business through a focus on information systems; creation of a system, in order to effectively manage the business, and determining the Bank risk appetite. However, some challenges ahead, including the lack of comprehensive guidelines in this regard by the supervisory authority and lack of necessary infrastructures in order to integrate information and processes, and lack of unity of banks in the implementation of GRC approach, have created restrictions on the establishment of this approach in the country's banking system. Hence, in order to strengthen and implementation of GRC in the banking system, proposes are provided in separate with the external (the Central Bank of Iran) and internal (bank) factors:

Central bank of Iran

Development of principles and operating procedures of GRC, according to international standards, such as the principles developed by the Basel Committee and the Islamic Financial Services Board, and communicating it to the Bank;

-Reviewing the organizational structure of the banks, according to international standards of corporate governance, risk management and compliance;

-Determine the board members' competency of banks, based on the duties description and specified responsibilities in the principles of corporate governance, risk management and compliance;

-Increased cooperation and effective exchange of information with regulatory authorities of other countries and better use of their experience in implementing GRC;

-The separation of ownership from management in public banks; now, in these banks, the Board of Directors is responsible for policy formulation and monitoring its implementation due to the unattainable content of ownership from management and the impact of environmental factors, and only, a legal obligation causes respecting these policies.

-The establishment of operational audit to assess the performance of managers and develop Accounting Standards, in terms of risk.

- Changes in the composition of the board of directors and committees in banks, in order to use non-executive directors, with the aim of increasing the role of oversight and more autonomy in decision-making managers;

-Increase central bank supervision indicators in order to ensure the effective implementation of GRC approach;

Iranian Banks

-The formation of the corporate governance committee, so that the committee reconsiders the duties description of relevant committees at the bank and monitors the implementation and functioning of committees.

-Integrating the activities of the Bank Committee, to establish the GRC.

-Implementing a comprehensive risk management at the bank, in order to measure, assess and control risks resulting from the activities of the bank;

-Increase the transparency of tasks and responsibilities in the organizational structure of the bank, to enhance the accountability of managers and employees;

- The establishment of a procedure for a full exchange of information at all levels of the organization,

-Develop an integrated model of GRC in accordance with the conditions and requirements of the banking system and Basel's standards;

- Use the appropriate framework for the establishment of GRC in the respective banks;

-Building a culture to support and guarantee of adapting the GRC approach from the organization and at the Board of Directors level;

- The use of a common language and literature in designing processes and activities of the organization;

-Manpower training and use of advisory services, foreign experts, in the field;

References

A MaturityModel for Integrated GRC. (2016). August,OCEG

Bahrami, Mahnaz; Amin Azad, Amir Hossein (2008). Localization Strategies for effective corporate governance in the banking system of Iran. Tehran: Central Bank of the Islamic Republic of Iran, the General Directorate supervision of banks and credit institutions, administration and regulation of banking.

Caramanolis-Cötelli, B. (1995). *External and Internal Corporate Control Mechanisms and the Role of the Board of Directors: A Review of the Literature.* Institute of Banking and Financial Management.

Falah Shams, Mirfeizi, & râşnov, Mehdi. (2008). credit risk management in banks and financial institutions (the concepts and models), Faculty of Economics.

GRC capability Model/OCEG red book

HasasYeganeh, Yahya (2005). Corporate governance in Iran. *The systems of corporate governance, accounting monthly, quarterly* SAS.169.

Hassanzadeh, Ali. Corporate Governance in Banks. *New Journal of Economics, 133*, 74-86.

MomenVaghefi, Nooshin. (2015). The integrated establishment of GRC. The fifth annual conference on electronic banking and payment systems, Tehran, Milad Tower International Convention Center.

Sawicki, arl. *American Express Kathleen Randall, RSA Archer GRC Program Best Practices& Lessons Learned*, EMC Corporation.

Tehrani, Reza Fallah Shams, & Mir Fallah. (2005). design and explanation of the credit risk in the banking system. *Journal of Social Sciences and Humanities,* Shiraz University.

Vicenta,p, & daSilva,M.M.(2011). A conceptual model for integrated governance, risk and compliance. In *Advanced Information systems Engineering* (pp.199-213). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21640-4_16

Notes

Note 1. GRC stands for the Latin words corporate governance, risk and Compliance of rules and standards.

Note 2. Razak et al. (2010)

Note 3. A system is called (Scalability) so that it could be usedproperly, practically and efficiently for a larger scale.

Note 4. Measures of performance are divided into three categories:

1. Key Result Indicators (KRIs): how is the performance at a certain point.

2. Performance Indicators (Pis): what should be fulfilled?

3 .Key Performance Indicators (KPIs): what you should do to increase the efficiency of organization.

Note 5. Business continuity Plan

Note 6. Information attachment means the GRC rules and principles not only should act integrally, but also increase efficiency and productivity and reduce costs.