Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-4 || July2023 || PP. 150-156 https://doi.org/10.55544/ijrah.3.4.19

Compliance Requirement for Dealing with Risks, Governance and IT Compliance

Gulwali Mohammadzai[1], Khalid Pashtoon[2] and Ilhamuddin Aini[3]
[1]Assistant Professor, Department of Finance and Banking, Faculty of Economics, Shaikh Zayed University, Khost, AFGHANISTAN.
[2]Assistant Professor, Department of National Economics, Faculty of Economics, Shaikh Zayed University, Khost, AFGHANISTAN.
[3]Master Graduated Student, Department of Finance and Credit, Faculty of Economics, Southern Federal University, Rostov-on-Don, RUSSIA.

Corresponding Author: Gulwali Mohammadzai

ORCID

https://orcid.org/0009-0003-8223-3165

www.ijrah.com || Vol. 3 No. 4 (2023): July Issue

Date of Submission: 05-07-2023	**Date of Acceptance:** 20-07-2023	**Date of Publication:** 10-08-2023

ABSTRACT

The common approaches for a compliance requirement are to manage and identify the risks that an organization faces and advise them on. This paper examined and analyzed the best ways for businesses to adapt and enhance different effective compliance regulations and the key issues that must be enforced by businesses. These approaches help the organizations identify the simplest ways of compliance guidelines for organizations in order to manage and govern the risks. Due to a massive revolution of technology it is important to notice the IT compliance. Our findings show that IT compliance adaption will help the organizations to better manage the risks and to reduce the cost of the compliance procedure.

Keywords- Compliance, Compliance Management, Risk, Compliance regulations, IT, IT compliance, Governance.

I. INTRODUCTION

Governance and compliance are two important concepts that organizations must consider in order to operate effectively and manage risks. Governance involves the oversight role and process by which companies manage and mitigate business risks. It includes several key elements, such as the definition and communication of corporate control, the establishment of main policies, enterprise risk management, regulatory and compliance management, and the evaluation of business performance. Compliance, on the other hand, refers to the processes and internal controls that ensure an organization meets the requirements imposed by governmental bodies, regulators, industry mandates, or internal policies. Compliance is crucial for organizations to avoid legal or reputational risks, and to maintain the trust of their stakeholders. By making compliance repeatable, organizations can sustain it on an ongoing basis at a lower cost. Overall, both governance and compliance are important components of effective risk management, and organizations must consider both in order to operate successfully and sustainably.[1]

IT compliance is crucial for managing and safeguarding information, including its acquisition, storage, security, availability, and protection. Internal compliance focuses on a business's policies, goals, and

[1] CPD for members in Commerce & Industry, Aug, 2018. "Governance, Risk and Compliance.

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-4 || July2023 || PP. 150-156 https://doi.org/10.55544/ijrah.3.4.19

structure, while external compliance focuses on customer satisfaction and protecting the company. Specialized tools are used continuously to identify, monitor, report, and audit to ensure compliance is achieved and maintained[2].

The increase in investment related to compliance is primarily due to regulatory mandates that have emerged in response to significant scandals in corporate history, such as Enron, WorldCom, and Socoete Generale. Compliance involves ensuring that business processes, operations, and practices adhere to specific norms and standards. The introduction of regulations such as the Sarbanes-Oxley Act of 2002, Gramm-Leach-Bliley Act of 1999, and Health Insurance Portability and Accountability Act of 1996 have made regulatory compliance a central focus for many organizations. These regulations aim to improve transparency, accountability, and trust in business operations, while also protecting stakeholders' interests and mitigating risks. As a result, organizations have increased their investment in compliance to ensure they meet these regulatory requirements.

Organizational departments such as finance, administration, and information systems are impacted by compliance changes. Investment in compliance is mandatory to maintain business operations, as noncompliance with governmental, legal, and regulatory requirements can have severe consequences for organizations[3].

All organizations, required to operate with strong strategies, norms, standards and practices regardless to the size or type of their activities[4].

Organizations face the challenge of not only understanding governance, risk, and compliance (GRC) concepts, but also implementing them effectively to achieve efficient and adequate results. A complex regulatory environment, accountability concerns, and increased business complexity have led organizations to adopt a variety of GRC innovations across their entities. However, these initiatives may be uncoordinated, leading to increased overall business risk. Additionally, parallel compliance and risk initiatives can result in duplicated efforts and increased costs. GRC processes, through enforcement, monitoring, and control, have the ability to coordinate and integrate these initiatives, providing a more efficient and effective approach to GRC management.

[2] Abdullah, Norris Syed, Marta Indulska, and Sadiq Shazia. "A study of compliance management in information systems research." (2009).
[3] Coglianese, C. and Nash, J., 2020. Compliance management systems: Do they make a difference?. *Cambridge Handbook of Compliance (D. Daniel Sokol & Benjamin van Rooij eds., Cambridge University Press, Forthcoming), U of Penn, Inst for Law & Econ Research Paper*, (20-35).
[4] Ghirana, Ana-Maria, and Vasile Paul Bresfelean. "Compliance Requirements for Dealing with Risks and Governance." *Procedia Economics and Finance* 3 (2012): 752-756.

II. LITERATURE REVIEW

A study in compliance management (Norris, Indulska, and Shazia, 2009) is proving the increasing attention in recent years given by research journals and papers. The scholar community want to shift the view about compliance that was often considered a burden into a business opportunity. Many authors (Norris, Indulska, and Shazia, 2009; Lu, Sadiq, and Governatori, 2010; Shazia, Governatori, and Namiri, 2007) agree that *compliance* is about ensuring that the business processes, operations and practice are in accordance with a set of norms.

Compliance management is defined as all the mechanisms used to help the organizations to non-violate any regulations. Regulatory compliance has attracted much investment by organizations across the globe (Braganza & Franken 2007). According to the result of a survey that done by Economic Intelligence Unit shows that the usage of IT in compliance is growing rapidly in monitoring business activity that is heavily reliant on technology, such as privacy and security. Governance, Risk and Compliance is a term that applied to products and help companies dealing with areas as far as Sarbanes – Oxley compliance, risk management and IT governance (Kelly, 2009).

III. METHODOLOGY

This paper focused on Compliance requirements for Governance, Risks and IT compliance for organizations. In this research different model of GRC requirements were selected and analyzed. The role of IT compliance also fully described. The data for this study was obtained mainly from secondary sources, World Famous journals, Reports, Executive Opinion and Literature review.

IV. RESEARCH PROBLEM AND OBJECTIVE OF THE STUDY

In this paper we tried to find the best ways for business that can help them to analyze, manage and identify the risks that the organizations face with them. The risks usually defined that an outcome or investment result will differ from expected return. This paper will offer the best ways for businesses to adapt various effective compliance regulations and important issues that should be implement by businesses.

V. SUBJECT OF THE STUDY

Subject of the study is Compliance Requirement for Dealing with Risks, Governance and IT Compliance. Since the risks treat organizations in different situations the importance of the compliance is gaining due to the existence of these risks. There is a

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-4 || July2023 || PP. 150-156 https://doi.org/10.55544/ijrah.3.4.19

need for the authorities and responsible to take strict steps against non-compliance firms. In order to be able to reduce the possibility of different risks and frauds which is very harmful and intolerable for entities.

VI. GOVERNANCE FRAMEWORK

Corporate governance is the process by which organizations manage business risks, including elements such as communication, corporate control, regulatory compliance, and enterprise risk management (Kim & Nofsinger, 2015). Corporate control refers to the authority to make decisions about operations and strategic planning, including acquisitions, financial decisions, and marketing. Regulatory compliance ensures that organizations comply with relevant policies, laws, and regulations (Kim & Nofsinger, 2015)[5].

Enterprise Risk Management (ERM) is a business strategy that involves assessing, identifying, and preparing for potential risks that may impact an organization's objectives and operations. This includes both physical and figurative disasters (Kim & Nofsinger, 2015)[6].

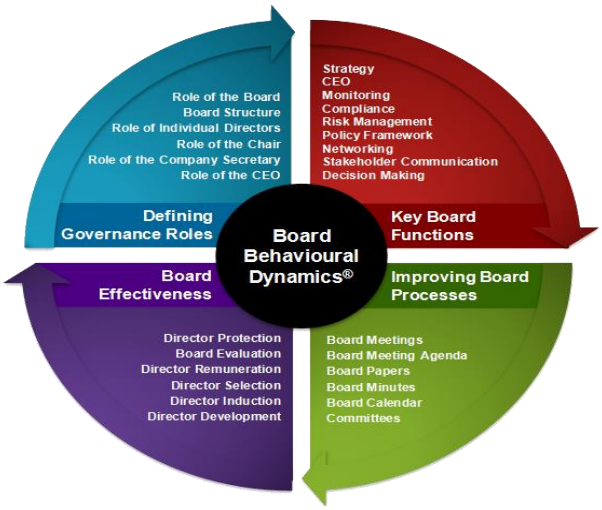

Fig. 1. Governance Framework

Source: https://www.pngkey.com/detail/u2r5u2t4e6i1r5y3_corporate-governance-practice-framework-corporate-governance-framework-template/

This picture shows the four important aspects of a healthy governance framework. These key functions must be used in action by all enterprises regardless of the size and type of them. It will result to mitigate the risk and increase the internal and external control by the board of directors.

VII. RISK MANAGEMENT FRAMEWORK

Risk Management enables organizations to appraise all related business and regulatory risks and control, monitor actions in a planned manner. With the recent increase in regulatory mandates and increasingly activist shareholder's lots of organizations become sensitized to indemnify and manage the risk areas in their businesses whether it is operational, financial, IT, brand, or other related risks.

Besides, the entire risks are no longer considered the sole burden of executive specialists and the boards demand visibility into exposure that they can effectively lead the organizations long-term strategies[7].

Finally, companies are looking to systematically identify, prioritize, measure, and respond to all kinds of risk in the business and then try to manage any of the related exposures.

Fig. 2. Risk Management Framework chart

Source: https://www.aviva.com/investors/risk-management-framework/

This figure shows different frameworks that how risk management can do its jobs. First of all, it's necessary to identify the risks that could potentially prevent the programs, activities or investment from achieving its objectives. Risk measures shows the statistical or historical predictors of probable risks. Risk manage include identification of what could go wrong, the evaluation of which risks should be deal with and the implementation strategies to deal and prevent those risks. Monitoring of risks helps the authorities to control and keep track of the identified, residual and new risks.

[5] Reference: Kim, K. A., & Nofsinger, J. R. (2015). Corporate governance. Pearson.
[6] Reference: Kim, K. A., & Nofsinger, J. R. (2015). Corporate governance. Pearson..
[7] World Health Organization, 2022. Ending the neglect to attain the sustainable development goals: a rationale for continued investment in tackling neglected tropical diseases 2021–2030.

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-4 || July2023 || PP. 150-156 https://doi.org/10.55544/ijrah.3.4.19

This stage also monitors the execution of planned strategies for the identification and evaluation of risks and their effectiveness. The final stage is risk reporting. The reporting procession can be on a quarterly basis, in a case if required it can be reported to the Executive Board outside of the quarterly process.

VIII. COMPLIANCE FRAMEWORK

Compliance ensures that the organizations have the internal control and processes to meet the requirements that imposed by governmental bodies, regulators, industry mandates, or internal policies. [8]

Compliance is not a one-time event that organizations realize that they need to make it into a repeatable process, thus that they can continue to hold compliance with that regulation at a less cost than for the first. The compliance process enables organizations to make compliance repeatable and therefore enables them to maintain it on an ongoing basis at a lower cost.

The Compliance Framework has three pillars:

1. **Inform** (ensuring staff are aware of their obligations and the legislative changes that may impact their business unit's activities);
2. **Comply** (an annual compliance declaration by Deputy Vice Chancellors, Provost, and the Vice Chancellor); and
3. **Assure** (internal and external audit and review activity) - providing a formal approach to continuous improvement. There will also be regular monitoring and review of the Framework's performance.[9]

Fig. 3. Compliance Framework

Source: http://grierconsulting.com/index_2Comp.html

A compliance framework is a set of guidelines and best practices that organizations use to achieve regulatory requirements and improve business processes. Internal auditors and other internal stakeholders can use the compliance framework to evaluate an organization's internal controls, while external auditors can use it to verify a company's internal controls.

IX. COMPLIANCE APPROACHES

9.1. Theoretical and Practical Approaches

To certify compliance with regulations, companies undergo expensive audit processes. To manage costs, companies can separate projects for each type of regulation they must comply with. For example, financial disclosure regulations such as the Sarbanes-Oxley Act of 2002, quality requirements such as ISO 9000:2008, data security regulations such as the Payment Card Industry Data Security Standard (PCI DSS), and ecological regulations such as the Waste Electrical and Electronic Equipment (WEEE) compliance can each be managed separately (Marwane et al., 2009)[10].

Dealing with numerous regulations by considering them individually or departmentally can result in a fragmented view of compliance, as regulations often overlap and influence each other. While audits are commonly used for compliance checking, research suggests that compliance should be considered at the business process level, as these processes control all value-adding activities in a company. Several studies have identified a gap between business processes and compliance obligations within companies (Schumm et al., 2010; Governatori & Rotolo, 2008; Comes et al., 2006).

The important point that identified by Guido and Shazia, 2009 is that compliance can be seen as a connection between the specifications for execution of a business process on one hand and the specification regulation of a business on the other hand. Checking compliance contain of verifying that there is no execution of the processes to crack the established norms. For enabling such verification, it is necessary to have a formal explanation of the propositions, that is very hard for common manager to understand it.

9.2. Common issues in compliance approaches

As with the audit method, demonstrating the dependence of business modelling might recommend some redundancy tests as some operations more times against the same requirements. This is generally occurred with IT operations which have effect to three types of business processes: operational, management and supporting processes. As an example, one directive

[8] https://reciprocitylabs.com/resources/what-is-a-compliance-framework/

[9] https://www.jcu.edu.au/policy/procedures/corporate-governance-procedures/compliance-framework

[10] Marwane, W., Stein, S., Markovic, I., & Pulvermaller, S. (2009). Compliance management for small and medium-sized enterprises. In Proceedings of the 15th Americas conference on information systems.

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-4 || July2023 || PP. 150-156 https://doi.org/10.55544/ijrah.3.4.19

from financial reporting could require building and sustaining a safe and secure network which is also essential in PCI (Payment card industry) compliance.

Organizations are subject to supply regular updated on compliance and this imply a change from a regular review to a ceaseless assurance. Researchers Marwane, Stein, Markovic, and Pulvermaller, 2009 stimulate the need for automation in compliance management and the clue in getting this consists in using the IT.

As the using of IT infrastructures are used by companies for collection of data, control implementation and analytical capabilities, this is natural that compliance checking also turning to technology. Third party software sellers are already providing solutions ready to use.

In a case the compliance automation is addressed by hard coded measures than it is a source of high costs as it is expensive to change multiple guidance. Further, it also enhances the problem of trust in the completeness and correctness of normative requirements modelled by software solution Bamberger, 2010. Technology systems intended to control risks themselves can create different type of risks by covering some illegalities.

Regulations have all their base on the urgency to protect shareholder like suppliers, employees, customers, government, any other interested parties from risks. Although, there are a lots of research on each spate domain like risk management, governance and compliance as separate topics, a study by Racz, Weippl and Seufert, 2010 emphasizes that they could also be viewed in an integrated way. Some framework created and designed to reunite them which currently promoted by important organizations. One is GRC capability Model GRC, 2009 which developed by Open Compliance and Ethic Group (OCEG), or the Unified Governance Framework (UGF) proposed by IBM Pfitzmann, B. and Powers, C. and Waidner, M. 2007.
The approach that should integrate the advantages found in both practical and theoretical methodologies while reducing the limitations:

- A holistic view- for example if we have M normative statements and N system to apply them, it will end with a result of MxN mappings because for each system we have to check each regulation. This is happening in audits (Practical compliance assessments) but also in business modelling (research compliance approaches), there must be a layer between regulations and their actual enforcement that could be use a shared language, semantics for capturing and formalizing all the compliance requirements.
- Easy to understand and enforce – for adoption by majority of organizations its necessary to have a conceptual model that could be consulted at any time.
- Companies have to be able to response if they a comply with requirements in specific situations even if they have not encountered yet. This is also necessary due to many directives include time constrains such as duration limitations or responds which requested in a certain time.
- To be able to quickly address changes – in real time the compliance requirements are including a directive about the frequency of the updates over the performed reviews.
- To be cost effective and reusable.
- Have to suggest traceability from regulations to system – actually this is a new directive which maintain a majority of regulations in order to show how compliance was achieved. If it is not achieved anyhow but it has to be economical and time subjective.

9.3. IT Compliance

The role of IT compliance is continuing to grow as the electronic sharing and storing of information impacts department such as human resources, finance and operations which all relates on the services of IT in their information collection, diffusion and reporting. [11]

IT compliance taking proper control of and protecting information, including how it is stored and obtained, how it is maintained, its accessibility (how it is distributed externally and internally), and how the data is protected. The internal compliance functions around the goals, policies and organizational structure of the business. External attention contains satisfaction of the customer or end users while protection of company and end user form harm. Specialized tools are using for continuation of monitoring, identifying, reporting and auditing in order to achieve and remain in compliance.

In connection to IT compliance, IT Governance is the function to manage and address the overriding strategical, technical and procedural processes. IT governance is a subset of the overall corporate governance process and is overseen in most cases by the appropriate C-suite professional such as Chief Compliance Officer (CCI) with increasing cross-functional responsibilities from a Chief Technical Officer (CTO).[12]

9.4. Requirements for IT Compliance

For IT compliance, there are many well-known standards such as COSO, 1992, COBIT, 2007, ISO/IEC, 2009, ITIL 2001, CC, 2012 common criterial that to the IT infrastructure can address a bundle of regulatory or corporate requirements including SOX or PCI. COSO framework designed for internal auditing and it evolve to support information system audits. COBIT standards allows to create policies for information control to consider that IT have to deliver all the necessary information for a company to reach its objectives. ISO 27000 is set of standards which include the

[11] Racz, Nicolas, Edgar Weippl, and Andreas Seufert. "A process model for integrated IT governance, risk, and compliance management." *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*. 2010.
[12]Marketing, Evelyn Uhlrich Product. "Software AG Martin Kling Business Development." *Software AG "Governance, Risk and Compliance an Integrated Approach for Improving Oversight and Efficiency" February* (2012).

Integrated Journal for Research in Arts and Humanities
ISSN (Online): 2583-1712
Volume-3 Issue-4 || July2023 || PP. 150-156 https://doi.org/10.55544/ijrah.3.4.19

specifications for information security management system and also this standard provides the control objectives for information security. ITIL also offered a family of practices for IT services management, to focus on aligning them to the business needs. Common Criteria (CC) is a framework which primary aims is to establish a common evaluation for the IT products and services from the security point of view.

A company which has been truly interested to apply for one of these standards and not just obtain the certification by designing and enforcing procedures, policies, controls will definitely comply with other requirements or even future changes in the current ones.

Applying one of these standards results in:

- Assess risks regarding to IT
- Create a control environment
- Design and implement controls and control processes
- Monitor the effectiveness of the controls in mitigating the risks

To prove control processes, a company can use control objectives that are formulated at a high level of abstraction and tailored to its specific purposes. Compliance performance can be measured using maturity models that assign levels from 0 to 5, corresponding to the non-existence of controls to the most optimized degree where automatic compliance is achieved. IT controls frameworks commonly use these models. However, failures in resource usage, access, or information disclosure may still occur in specific situations (Mellado et al., 2015)[13].

Compliance can be checked through IT solutions; the results are a function of the number of shortages found in the system. In some cases, if some limitations that are overridden were discovered, it is not necessary mean that organization is not in control of its processes.[14] That's why, the software should take into account what is useful for the organization, for matching the Governance, Risk and Compliance (GRC) unified perspective. [15]

9.5. IT Compliance Goals and Challenges

The main goal of IT compliance is to build a procedural, technical and strategic framework which provides the means for attaining and proving a company's legal and ethical integrity. To provide a defensible policy, mechanisms and procedures can help to avoid the following:[16]

- Damaging to corporate image standing or consumer trust [11]
- Lost revenue, market opportunity or stock value [11]
- Remediation consumption (fines, legal costs and judgments, purchased consumer protections, lost productivity and capital acquisitions). [11]

Although, to achieve these goals the organizations will face with many challenges. Firstly, the complexity and domain of new statutes are subject to interpretation. Since, the regulations themselves do not coming with a concrete roadmap, there are various industry-specific guideline and best practices are available which are providing clarity and guidance.

- Lack of employee education
- Shadow IT issues, such as personal mobile devices which circumvent corporate IT systems.
- Unauthorized applications
- Difficulties with service providers (could services and data centers)
- The role of social media
- Number of current regulations, updates and new laws.

X. CONCLUSION

This paper supported the need in which organizations address compliance as a business opportunity and emphasized over the advantages which it can bring rather than effects caused by non-compliance. Firstly, we started with defining Governance framework, Risk management framework and compliance framework. Then included the compliance concept and the compliance management which followed by explanation of practical and theoretical approaches. Both methodologies are altering the individual assessment of every regulation for the adoption of formalized specifications of regulations.

The paper enumerates the utmost important requirements in order to achieve compliance management and explains the essential role which played by IT for this. In this paper we have also considered the GRC in an integrated manner and which is contributing as well in increasing the interest for a consolidated solution.

REFERENCES

[1] Abdullah, Norris Syed, Marta Indulska, and Sadiq Shazia. "A study of compliance management in information systems research." (2009).

[2] Coglianese, C. and Nash, J., 2020. Compliance management systems: Do they make a difference?. *Cambridge Handbook of Compliance (D. Daniel Sokol & Benjamin van Rooij eds., Cambridge University Press, Forthcoming), U of Penn, Inst for Law & Econ Research Paper*, (20-35).

[3] CPD for members in Commerce & Industry, Aug, 2018. "Governance, Risk and Compliance.

[13] Mellado, D., Fernández-Medina, E., Piattini, M., & Ruiz, E. (2015). A systematic review of IT governance measurement. Information and Software Technology, 57, 187-211.

[14] https://www.smartsheet.com/understanding-it-compliance

[15] Spanaki, Konstantina, and Anastasia Papazafeiropoulou. "Analysing the governance, risk and compliance (GRC) implementation process: primary insights." (2013).

[16] https://www.skillcast.com/blog/top-10-compliance-challenges-2020

[4] Ghirana, Ana-Maria, and Vasile Paul Bresfelean. "Compliance Requirements for Dealing with Risks and Governance." *Procedia Economics and Finance* 3 (2012): 752-756.
[5] Marketing, Evelyn Uhlrich Product. "Software AG Martin Kling Business Development." *Software AG "Governance, Risk and Compliance an Integrated Approach for Improving Oversight and Efficiency" February* (2012).
[6] Marwane, W., Stein, S., Markovic, I., & Pulvermaller, S. (2009). Compliance management for small and medium-sized enterprises. In Proceedings of the 15th Americas conference on information systems.
[7] Mellado, D., Fernández-Medina, E., Piattini, M., & Ruiz, E. (2015). A systematic review of IT governance measurement. Information and Software Technology, 57, 187-211.
[8] Racz, Nicolas, Edgar Weippl, and Andreas Seufert. "A process model for integrated IT governance, risk, and compliance management." *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)*. 2010.
[9] Reference: Kim, K. A., & Nofsinger, J. R. (2015). Corporate governance. Pearson.
[10] Reference: Kim, K. A., & Nofsinger, J. R. (2015). Corporate governance. Pearson..
[11] Spanaki, Konstantina, and Anastasia Papazafeiropoulou. "Analysing the governance, risk and compliance (GRC) implementation process: primary insights." (2013).
[12] World Health Organization, 2022. Ending the neglect to attain the sustainable development goals: a rationale for continued investment in tackling neglected tropical diseases 2021–2030.
[13] https://reciprocitylabs.com/resources/what-is-a-compliance-framework/
[14] https://www.jcu.edu.au/policy/procedures/corporate-governance-procedures/compliance-framework
[15] https://www.skillcast.com/blog/top-10-compliance-challenges-2020
[16] https://www.smartsheet.com/understanding-it-compliance