Adoption of the COSO methodology for internal Sharīʿah audit

Said Bouheraoua and Fares Djafri
ISRA Research Management Centre, INCEIF University, Kuala Lumpur, Malaysia

Received 8 April 2020
Revised 30 August 2020
7 August 2021
26 April 2022
3 June 2022
Accepted 3 June 2022

Abstract

Purpose – Islamic financial institutions (IFIs) are required to establish a Sharīʿah Governance Framework (SGF) to strengthen their Sharīʿah-compliance mechanism and ensure that all relevant IFI regulations are in line with Sharīʿah rules and principles. Effective implementation of the Sharīʿah-compliance function will further promote stakeholder confidence, as well as the integrity of IFIs, by reducing Sharīʿah non-compliance risks. This study aims to examine the internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and explore the extent to which it can be incorporated in the Sharīʿah-compliance function of IFIs.

Design/methodology/approach – This study adopts a qualitative method of inquiry, utilizing the inductive method and content analysis to build comprehensive knowledge that will assist in exploring the framework of COSO methodology and the extent to which it can be adopted by IFIs.

Findings – The findings indicate that the existing frameworks of Sharīʿah governance, whether that of the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI) or Bank Negara Malaysia (BNM), need to be further developed. Therefore, the adoption of COSO methodology in the internal Sharīʿah audit of IFIs, as suggested by AAOIFI, is not only possible but desirable. The study also finds that the COSO framework places the highest priority on risk management in that it makes it an integral part of the decision-making process in all the institution's activities. As a result, incorporating the comprehensive COSO risk management structure within the Sharīʿah-compliance function will enhance risk management in IFIs.

Originality/value – This study highlights the importance of the COSO internal control framework and examines its components, principles and the possibility of its adoption by IFIs. The findings of this study are expected to contribute to enhancing the Sharīʿah-compliance function of IFIs.

Keywords COSO, IFIs, Internal control, Sharīʿah audit, Sharīʿah compliance, Sharīʿah governance

Paper type Research paper

Introduction

The development of the Islamic finance industry has led to the progression of the organisational structure of Islamic financial institutions (IFIs), especially in strengthening the concept of adherence to the principles and provisions of Sharīʿah (Islamic law).

Sharīʿah supervision and Sharīʿah audit are forms of administrative control to ensure that all operations and transactions carried out by IFIs are Sharīʿah-compliant. Given this importance, the Accounting and Auditing Organization for Islamic Financial Institutions (AAOIFI), in its ninth standard on governance, paid special attention to the Sharīʿah-compliance function, calling for the adoption of a comprehensive and integrated control system to manage the risks that IFIs may face. The standard identifies the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model as one of the advanced and comprehensive internal control methodologies and calls for incorporating the Sharīʿah-compliance function within the comprehensive COSO risk management structure (AAOIFI, 2019). This suggestion by AAOIFI triggered the concerns of industry experts on

ISRA International Journal of Islamic Finance
Vol. 14 No. 2, 2022
pp. 221-235
Emerald Publishing Limited
e-ISSN: 2289-4365
p-ISSN: 0128-1976
DOI 10.1108/IJIF-04-2020-0071

the implementation of the COSO framework for Sharī'ah audit. Several questions arise in this regard, including:

(1) How efficient and effective is the COSO methodology in achieving Sharī'ah oversight objectives?

(2) Is COSO's methodology in harmony with Sharī'ah principles and objectives?

(3) Is it possible to integrate COSO's methodology within the internal Sharī'ah audit process?

This research aims at explaining the COSO methodology, its components and principles and the extent to which it can be adopted within the internal Sharī'ah audit process of IFIs. For this purpose, this paper is organised as follows: the next section provides a review of the literature on the COSO methodology for internal Sharī'ah audit. It is followed by a discussion on Sharī'ah governance and its role and principles. The next section then deliberates on the COSO internal audit framework, its components and principles. Thereafter, Sharī'ah audit and its applications in IFIs are discussed. The key contribution of the paper lies in the deliberation on the extent to which the COSO methodology can be applied to the internal Sharī'ah audit processes of IFIs. The final section presents the conclusion and recommendations of the study.

Literature review

Significant literature is already in place regarding the application of the COSO framework of internal control in conventional finance. For instance, Rezaee (1995) explained the importance of a COSO report for internal auditors and urged them to work closely with management and external auditors. The findings revealed that COSO reports have a significant positive impact on the better recognition of the proactive role of internal auditors. Lawson *et al.* (2017) surveyed United States (US) accounting professionals, principally from large publicly traded firms, to examine views related to the framework and its impact on key areas related to internal controls. The results revealed that respondents view the COSO framework and its 17 principles as a set of rules for achieving effective internal controls. Likewise, Udeh (2019) explored the effectiveness of the COSO framework. The findings showed that timely adopters of the COSO framework continued to demonstrate fewer instances of auditor-reported material weaknesses than late-adopters.

Besides, comparative studies conducted on the implementation of the COSO framework show that major regulatory and standard-setting bodies' presentations of their internal controls are drafted based on the COSO model. This is reflected in the model developed by The Basel Committee on Banking Supervision for internal control of financial institutions and the Cadbury Commission's report; both models are mainly based on the COSO framework for internal audit (Briciu *et al.*, 2014).

IFIs have also recognised the importance of benefiting from the COSO framework in establishing internal Sharī'ah control. This realisation is supported by AAOIFI and other regulatory and supervisory bodies. AAOIFI decided to incorporate the framework in its Sharī'ah Standard of Governance Standard No. 9 on "Sharī'ah Compliance Function". AAOIFI stated explicitly that the Sharī'ah compliance chart is "developed in line with the five key pillars of the COSO integrated framework" (AAOIFI, 2019). The standard also stated in clause 38: "IFIs shall consider adopting a comprehensive internal control or enterprise risk management framework (e.g. those developed by COSO)". The same consideration of the COSO framework was presented in the AAOIFI Exposure Draft of Waqf Governance Standard, clause 56. The draft states: "The custodian shall also establish and cause to implement and follow a control framework in line with global best practices (e.g. the

Committee of Sponsoring Organizations of the Treadway Commission's (COSO's))" (AAOIFI, 2018). This is in addition to the incorporation of the framework by many IFIs in their Sharīʿah Governance Framework (SGF) and policy documents. Despite the importance given to the COSO framework, not much literature concerning its applications in Sharīʿah audit and control has been produced by researchers and industry practitioners.

In the Islamic arena, the studies conducted on the COSO framework can be divided into two categories. The first category stresses the general importance of COSO in Sharīʿah audit and its position in the internal Sharīʿah control undertaking. Hidayah (2014) proposed a modified triple line of defense for IFIs based on the COSO framework. Similarly, Zakaria *et al.* (2019) highlighted the importance of the implementation of the COSO framework in internal Sharīʿah control and cited the study of Shafii and Salleh (2010) as one of the first to discuss the Sharīʿah internal control system and to adopt the COSO framework in defining internal Sharīʿah control. However, the study did not comprehensively explain the framework, nor did it present any assessment from the Sharīʿah perspective (Zakaria *et al.*, 2019).

The second category is concerned with practical examination of the COSO framework either by evaluating its application in specific products or conducting empirical studies by interviewing stakeholders to assess its importance and the extent of its implementation in internal Sharīʿah audit. For instance, Aden Abdi (2017) examined the possibility of the implementation of the COSO framework in Islamic finance. The research concluded that although the COSO framework is useful for Islamic finance, it misses some essential elements related to internal Sharīʿah control, especially the Sharīʿah-compliance aspect and the party responsible for Sharīʿah compliance as well as the Sharīʿah supervisory board (SSB) as a line of defense. Yazkhiruni *et al.* (2018) interviewed chiefs of internal audit, managers of internal audit department, Sharīʿah committee members, external auditors and academicians on the implementation of the COSO framework in enterprise risk management and found that some respondents confirmed they are adopting the COSO framework. Likewise, Abd Rahman *et al.* (2018) stated that the COSO framework is considered an effective methodology as it contains all facets for ensuring an effective internal control system. This was supported by the final statement and recommendations of the Shura Eighth Sharīʿah Audit Conference, which was held in the Sultanate of Oman in 2019. The conference recommended the adoption of the COSO Sharīʿah audit framework as one of the most advanced and comprehensive internal control frameworks. Furthermore, the conference recommended that the entities working in the field of Sharīʿah consultancy and audit should provide professional support to Islamic financial institutions on how to adopt the COSO methodology in the internal Sharīʿah control system, develop the professional capabilities of the institutions' staffs by holding workshops and training programs and carry out the necessary technical studies that illustrate the practical application of the COSO framework (Shura, 2019).

From the above studies, it can be concluded that the efforts undertaken by researchers have focused on examining the efficiency of the COSO internal control framework and its importance for internal Sharīʿah control; however, they have not addressed its compliance to Sharīʿah requirements and how to incorporate it within the existing SGF of IFIs. This gap was highlighted in CIBAFI's comments on the "AAOIFI Exposure Draft on Governance Standard No. 9 on Sharīʿah Compliance Function" as follows:

> The COSO's pillars are defined in a purely secular context. If they are to be cited, therefore and in order to educate the SSB members and those charged with governance about their application to the Sharīʿah-compliance function, the standard should elaborate more on linking the COSO components to Sharīʿah requirements (CIBAFI, 2017, p. 5).

The present study goes beyond CIBAFI's concern about the secular context. It aims to undertake an in-depth examination of the extent to which the COSO framework complies with Sharīʿah principles and fundamentals and the possibility of adopting it within the SGF of IFIs.

Sharīʿah governance: its role and principles

Many definitions have been provided for governance in the conventional law context, including: the system by which companies are managed and their activities controlled (Alamgir, 2007). The National Bank of Egypt (2003) defined it as the aggregate "rules of the game" that are used to oversee the business from within and by which the board of directors (BOD) supervises it to protect the interests and financial rights of the shareholders.

It is worth noting that there is no difference between Sharīʿah governance and the governance of conventional companies except in terms of the law that governs them. Sharīʿah governance, as the name suggests, is derived from Islamic law while conventional governance is based on statutory laws. IFIs are required to have an SGF to strengthen their Sharīʿah-compliance mechanism and ensure that all relevant IFI regulations comply with Sharīʿah rules and principles. Successful implementation of the SGF will further elevate stakeholder confidence as well as the trustworthiness of the Islamic finance industry by decreasing Sharīʿah non-compliance risks. That will ultimately contribute to maintaining financial stability. Bank Negara Malaysia (BNM) provides a good benchmark in this regard as it places increased emphasis on ensuring that the operations of the Islamic financial system are in line with the SGF. Indeed, BNM has developed the SGF for IFIs with the main objective of enriching the function of the board, the Sharīʿah committee and the management in discharging their duties in matters relating to Sharīʿah.

AAOIFI also confirmed that governance in IFIs far exceeds the limits of governance in conventional institutions, given the additional social and religious dimensions of the former (AAOIFI, 2004). Likewise, the Islamic Financial Services Board (IFSB, 2009) expressed the concept thus: a set of legislative measures through which IFIs confirm that there is independent and effective Sharīʿah supervision for each of the following structures and processes:

(1) Issuing fatwas and related decisions governing the work of the financial institutions.

(2) Disseminating information related to these fatwas and decisions among the employees in Islamic financial services institutions who are responsible for monitoring daily activities.

(3) Internal Sharīʿah review and audit to verify the compliance of the transactions conducted in the financial institution with the Sharīʿah provisions.

(4) A yearly Sharīʿah review to confirm that the internal Sharīʿah supervision and audit were implemented appropriately and as required.

The mandatory nature of Sharīʿah governance in Islamic financial institutions

The mandatory nature of Sharīʿah governance for IFIs means that the decisions of the SSB are binding in Sharīʿah issues related to the bank, as is the achievement of the Sharīʿah principles included in Sharīʿah governance. These include justice, honesty, trustworthiness, accuracy, clarity, the prevention of inequity and the preservation of rights. Therefore, the SSB's role is more than consultative; rather, it includes guidance, supervision and oversight. This is clearly stated in the revised SGF for IFIs issued by BNM (2019). SGF 2019 obliges the SSB to be accountable for the soundness and accuracy of decisions related to business and risk practices. In this regard, the Sharīʿah committee shall inform the SSB about any Sharīʿah issue or matter that may affect the safety and soundness of the IFI. It is worth noting that the basic principle in Sharīʿah supervision of Islamic banks is oversight of the bank's business. It is not limited to developing products or following up on their implementation. Rather, it makes sure that all business and all aspects of the bank are in compliance with the principles and provisions of the Sharīʿah.

Similarly, AAOIFI has issued governance standards on SSBs which state that the SSB is assigned with the responsibility of reviewing, managing and supervising the activities of the IFI in order to ensure that its financial products and services are in compliance with the principles and precepts of Sharīʿah (AAOIFI, 2015). Likewise, it is stated in AAOIFI Sharīʿah Standard No. 29 that it is the duty of the SSB to submit fatwas to the bank based on the relationship that exists between them and that it is the duty of the institution to refer to the board on Sharīʿah matters. In principle, the seeker of a fatwa, in this case the bank, can exert the utmost effort to choose the best fatwas or opinions; however, the laws of these institutions require them to accept and implement the fatwas issued by their own SSBs (AAOIFI, 2007). AAOIFI (2007) emphasised that the bank is obligated to follow the decisions of the SSB and cannot refer to and adopt the decisions of other fatwa bodies without the permission of its own Sharīʿah board.

Based on the above, Sharīʿah governance is concerned with practices, systems, policies, procedures and measures by which the institution's performance is controlled and monitored and its problems addressed. This is where the interaction between governance and internal Sharīʿah oversight becomes apparent. It is a crucial part of the governance of IFIs that aims to ensure that the transactions undertaken by the institution are in compliance with the provisions of Sharīʿah. It also aims to reduce the risks of Sharīʿah non-compliance that Islamic banks may face. In this respect, Mashal (2015) stated that governance represents an evolution of oversight and is based on three main axes: moral behavior, the risk management process and the process of oversight and accountability. In addition, internal SSBs are vigilant in identifying Sharīʿah non-compliance risks, dealing with them and minimizing them. Since internal control is an important part of corporate governance, ensuring that the approved goals are achieved and that risks facing the institution are reduced, the next topic will address what internal control is and its principles and goals according to the COSO concept.

COSO internal audit framework

COSO was established in 1985 under the chairmanship of James Treadway, the former Commissioner of the US Securities and Exchange Commission. The Committee includes professional bodies working in the accounting and financial field in the United States of America (USA). It includes the five largest private sector organisations in the USA: the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), the Financial Executives International (FEI), the American Accounting Association (AAA) and the Institute of Management Accountants (IMA). Collectively, they are called COSO in consideration of their funding provision to the Committee. The Committee was commissioned to produce an integrated and comprehensive design for internal control that came to be widely adopted in the USA (Uwadiae, 2015). This framework, known as the COSO framework, was designed to assist companies in establishing, correcting and improving the internal control system. Internal control, according to this framework, is considered important for the organisation's operations and financial reports and cannot be neglected because it determines the quality of the financial statements. It provides "reasonable assurance" that the amounts presented in the financial statements are correct and establish a reliable basis for making sound decisions (COSO, 2013).

The application of the internal control framework, according to the COSO concept, provides a solid basis for determining the degree of assurance provided by the regulatory controls designed at the institutional level. COSO defines internal control as:

> a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance (COSO, 2013, p. 3).

This definition reflects some of the basic concepts of internal control, namely:

(1) It is not an end in itself but a means to achieve goals.

(2) It is not just policies, procedures and systems but the actions that people take at every level of the organisation to affect internal control. Hence, it must be accomplished by competent and qualified persons.

(3) It does not provide an absolute assurance but, rather, a reasonable assurance regarding the institution's achievement of its objectives to the management and the BOD.

Besides, the objectives of internal control, according to the COSO framework, are as follows:

> *Operations objectives:* They relate to the efficient and effective use of all the entity's resources, including operational and financial performance goals and safeguarding assets against loss.
>
> *Reporting objectives:* They relate to internal and external financial and non-financial reporting directed at the use of what is produced and its documentation with reliable and transparent reports submitted to the management.
>
> *Compliance objectives:* They relate to compliance with the laws and regulations that the organization is subject to (COSO, 2013, p. 3).

In light of the above, it is clear that internal control, according to the COSO framework, is a comprehensive system designed to help achieve the entity's goals through the efficient and effective use of all the institution's resources. It does so through specific criteria, concepts and principles that are used to evaluate the internal control system. The next section examines the development of the COSO framework.

Development of the COSO framework

As previously mentioned, the main work assigned to COSO is to design an integrated framework to help companies establish, evaluate and improve the internal control system. The first version of the internal control framework was issued in 1992 and became widely accepted, particularly in the USA. In 2013, a revised and refined version of the COSO internal control framework was issued, containing the components applied under the COSO framework of 1992 with the addition of a set of principles and concepts. With regard to risk management, in 2004 COSO issued the integrated risk management framework. An updated version was issued in 2017 titled "Enterprise Risk Management (ERM) Integration of Strategies and Performance" (COSO, 2017). Since the subject of this research relates to internal control, it will focus on the stages of the development of internal control for the COSO framework.

COSO internal control framework – 1992 edition

The first version of COSO framework for evaluating and activating the system of internal control, issued in 1992, was based on five interrelated components: control environment, risk assessment, control activities, information and communication and monitoring activities. The overall objective of this framework was to provide reasonable assurance of achievement of the institution's goals at the following levels: effectiveness and efficiency of operational processes, reliability of financial reports and compliance with laws and regulations.

COSO internal control framework – 2013 updated version

Since the introduction of the first COSO framework in 1992, several amendments have occurred in the working environment and the organisational and operational laws of

institutions. This prompted COSO to review and amend the COSO framework in accordance with developments in the internal control system. In 2013, the revised and improved COSO internal control framework was issued. It contains the same components applied in the COSO 1992 framework along with the addition of a set of 17 principles that represent the basic concepts of the five control components that are relied upon in evaluating the internal control system (COSO, 2013).

Table 1 summarises the five components and 17 principles of internal control according to the COSO 2013 framework. The COSO 2013 framework assumes that these 17 principles work with one another in an integrated dynamic framework to reduce risks to reasonable and acceptable levels. The 17 principles are further supported by a set of 87 points that must also be given due attention. They represent the instructions that help design the implementation of the internal control procedure and evaluation of whether these principles have been adopted and used (Deloitte, 2014). It thus results in an effective internal control system.

The revised COSO 2013 thus focused on the risk management process. This reflected the realisation that it is important to shift risk management from a separate or occasional activity distributed among a number of the institution's units to an efficient, integrated management activity. In addition, the COSO 2013 framework indicated that risk management is an integral part of the decision-making process in an entity's activities and is crucial for achieving goals and improving performance. It indicated that an effective internal control system is not simply a matter of strict adherence to policies and procedures; rather, it goes beyond that to the exercise of judgement and discretion. This is a relative matter that requires competence on the part of those carrying out the work. The BOD, executive management and employees throughout the institution need to use their judgement to define the necessary and effective control limits. Likewise, their exercise of judgement and assessment of matters are used on an ongoing basis to develop the control system at the institutional level.

Sharīʿah audit and its applications in Islamic financial institutions

Before evaluating the COSO methodology or framework for Sharīʿah audit, it is necessary to present the methodologies of the most prominent supervisory and oversight bodies regarding internal Sharīʿah audit. As the limitations of this paper do not allow for the study of many models, only AAOIFI's and BNM's methodologies on Sharīʿah audit will be presented.

AAOIFI's internal Sharīʿah audit approach

AAOIFI has examined Sharīʿah audit in its Governance Standard for Islamic Financial Institutions (GSIFI No. 3). It defines internal Sharīʿah audit as the examination and evaluation of the institution's commitment to the provisions and principles of Sharīʿah and the fatwas, guidelines and instructions issued by the institution's SSB. Accordingly, internal Sharīʿah audit is an essential part of the organs of governance of the IFI and it is based on a set of general requirements that include:

Independence and objectivity: the organisational status of the internal Sharīʿah control shall be sufficient to accomplish its responsibilities. This is achieved by placing internal Sharīʿah control in the organisational structure at a position no lower than the level of the Internal Control Department. Further, the internal Sharīʿah control personnel are to receive full and continuous support from the management and the BOD. On the other hand, objectivity includes independence of thought and attitude that assist internal Sharīʿah audit to reach objective conclusions based on the work the internal Sharīʿah auditors have performed and its results. Therefore, the independence and objectivity of the internal Sharīʿah auditors are vital for public confidence. This will ultimately promote the objectives of Sharīʿah (*maqāṣid al-Sharīʿah*) which aim at realizing human wellbeing

Components	Description of the components	Principles
Control Environment	Control environment represents the philosophy and vision of the institution, or it is the governance culture of management, which impacts on the effectiveness of the other components of internal control. It denotes a set of standards, processes and structures that the organisation relies on to implement internal control. It includes the integrity and ethical values of the institution and the standards that enable the board of directors to carry out its responsibilities in overseeing the governance and organisational structure and in defining powers and responsibilities	(1) The organisation demonstrates a commitment to integrity and ethical values (2) The BOD demonstrates independence from management (3) The BOD establishes structures, reporting lines and appropriate responsibilities in the pursuit of objectives (4) Commitment to attract, develop and retain competent individuals (5) Holding individuals accountable for their internal control responsibility
Risk Management	It is the possibility that an event will occur and adversely affect the achievement of [an organisation's] objectives. It indicates that each organisation may face a variety of risks, external and internal. The assessment of risks, according to the COSO concept, is a continuous dynamic process for identifying and assessing the risks that threaten the achievement of the institution's goals	(6) Specifying objectives with sufficient clarity to identify and assess risks (7) Identifying risks across the entity and analyzing them to determine how they should be managed (8) Considering the potential for fraud as a possible risk (9) Identifying, evaluating and analyzing changes that could significantly impact the system of internal controls
Control Activities	Control activities are procedures established through policies and arrangements that help ensure the implementation of management directives to mitigate risks related to the achievement of the entity's goals	(10) Selection and development of control activities to mitigate risks (11) Selection and development of technology-dependent general control activities (12) Deployment of policies that define what is expected and procedures that implement them
Information and communication	It refers to the continuous and iterative process of providing, sharing and obtaining the necessary information. Communication is the means by which information is disseminated to all departments of the institution	(13) Obtaining and using relevant and credible information (14) Internal communication by disseminating information internally (15) External communication on matters affecting the conduct of internal control
Monitoring activities	Monitoring activities are carried out by either a continuous or discontinuous evaluation process, or a combination of them, to ensure that each of the five internal control components exists and works appropriately	(16) Conducting continuous or separate evaluations (17) Evaluating and communicating deficiencies of internal control

Source(s): COSO (2013)

Table 1.
Components and principles of COSO 2013 framework

(*maṣlaḥāh*) and preventing harm and difficulties (*māfsādāh* and *māshāqqāh*) to the public and the economy (Algabry *et al.*, 2020). In line with this, IIA in its standards has considered independence and objectivity as part of the internal auditors' framework. According to IIA (2017), independence means freedom from incidents that intimidate the ability of internal

audit activity in carrying out its obligation in an impartial manner. In contract, objectivity means the assessments and decisions of an auditor are not affected by any compulsion and remain neutral. It is in this regard that the internal Sharīʿah auditor must confirm that his evaluation and judgement in arriving at a Sharīʿah decision or advice is not affected by his other professional commitments and that it is free from any factors which may impair the exercise of his professional objectivity. As such, the internal Sharīʿah auditor must put in place a vigorous methodology to perform his decision-making and be responsible for the quality and accuracy of his decisions or advice.

Professional proficiency: This is achieved by good recruiting practices, supervision of internal Sharīʿah control, adherence to the code of ethics, proper knowledge, skills and discipline, continuous education and training and the necessary professional care (AAOIFI, 2015). Accordingly, internal Sharīʿah auditors shall be competent and shall have appropriate educational background and training relevant to the fulfilment of their roles and responsibilities. They must also keep up to date with developments that may take place in the Islamic financial business.

As for the scope of work of internal Sharīʿah audit, it shall comprise the examination of the adequacy and effectiveness of the IFI's system of internal Sharīʿah control and the quality of performance in carrying out assigned responsibilities. More specifically, the roles of the internal Sharīʿah auditor include the following (AAOIFI, 2015):

(1) Planning each of the Sharīʿah internal oversight tasks by collecting the information related to the activity to be monitored. Examples include:
   - Determining the objective and scope of internal Sharīʿah control;
   - Obtaining all fatwas, guidelines and instructions of the SSB, the results of internal and external Sharīʿah supervisory for the previous year and relevant correspondence, including correspondence with supervisory and oversight bodies;
   - Preparing the resources needed to carry out internal Sharīʿah control;
   - Conducting a survey of the parts that must be stressed in the internal Sharīʿah control, as appropriate, with a view to identifying activities, risks and parameters of control and inviting the monitored bodies to submit their observations and proposals;
   - Preparing internal Sharīʿah supervision programs;
   - Determining the method and date for reporting the results of internal Sharīʿah supervision;
   - Having the internal Sharīʿah supervision action plan approved by the authorised entities, including the institution's SSB.
(2) Examining and evaluating information related to internal Sharīʿah supervision;
(3) Attaching an objective report on the results of internal Sharīʿah supervision;
(4) In case measures have been decided upon, based on the final results of internal Sharīʿah supervision, follow-up must be done to ensure they have been implemented. This is necessary to prevent the recurrence of cases of non-compliance with instructions.

BNM internal Sharīʿah audit approach

BNM's SGF adopts a comprehensive approach to Sharīʿah audit. Its definition of Sharīʿah audit (BNM, 2019, p. 18) affirms that internal Sharīʿah audit operates within a comprehensive approach and falls within the framework of Sharīʿah supervision that aims to comply with the

provisions of Sharīʿah and that it works in integration with Sharīʿah risk management. BNM stresses that effective management of the risks of Sharīʿah non-compliance relies heavily on:

> a comprehensive and integrated approach to enterprise-wide risk management, which integrates risks arising from Sharīʿah non-compliance alongside other risks such as credit, market, operational and liquidity; and the effective integration of control functions under Sharīʿah governance and oversight arrangement of the risk management, compliance and internal audit at the entity-level and group-level (BNM, 2019, p. 16).

As part of the efforts for managing and controlling risk associated with Sharīʿah non-compliance events, the SGF 2019 reinforces the internal control function for effective management of such risks. Unlike the SGF 2011 framework, which introduced Sharīʿah research as an independent function, SGF 2019 assigns the research task to the secretariat of the Sharīʿah committee. It is evident through the review of the updated SGF 2019 that the updated SGF seeks to integrate Sharīʿah non-compliance risk matters with enterprise-wide risk management. This entails the IFI considering Sharīʿah non-compliance risk along with other risks such as market, credit, liquidity and operational. In addition, SGF 2019 moved further towards end-to-end Sharīʿah compliance by stressing the importance of spreading Sharīʿah-compliance culture within all aspects of the IFI. This involves embracing an appropriate "tone from the top" for the sake of communicating the importance of adherence to Sharīʿah requirements with all organisational levels. The updated SGF 2019 has also introduced and discussed in detail guidelines related to transparency and disclosure. Accordingly, the IFI will be required to present information about Sharīʿah governance, policies and practices in the annual report on its website. The report should also include the Sharīʿah committee's decision on the extent to which the IFI complies with Sharīʿah rules and principles. The disclosure requirements are applicable even for an IFI operating as an Islamic window. As a result, it is expected that the new SGF 2019 will further enhance the oversight responsibility of the BOD and all other key organs concerned in the implementation of Sharīʿah governance.

In view of the above, the internal Sharīʿah audit is closely related to the topic of risk management. They are the two main components of compliance with Islamic law and the key defense lines to ensure the safety of the institution. Risk management represents the second line of defense to control Sharīʿah risks while Sharīʿah audit represents the third line of defense to identify errors and Sharīʿah violations that occurred in the institution and to take corrective action and avoid their recurrence. According to BNM (2019, p. 16), Sharīʿah risk management is: "a function that systematically identifies, measures, monitors and reports Sharīʿah non-compliance risks to prevent any Sharīʿah non-compliances". This systematic way of controlling the risks arising from non-compliance with the Sharīʿah makes the institution able to continue its operations without exposing it to undesirable levels of risk. BNM (2019) further explained: "Sharīʿah risk control and management must be part of an integrated framework for risk management in the organisation." Also, given the professionalism and sophistication of risk management in Sharīʿah matters, this job should be done by risk management personnel who have appropriate qualifications and knowledge in risk management, as mentioned in BNM's SGF (BNM, 2019, p. 17).

Although some opinions discuss the Sharīʿah risks that the institution must manage as if they are a separate category of risks, they actually enter into all of the financial institution's activities. They include: product or model risks, marketing and distribution risks, organisational risks, investment risks, human resource risks, operational risks and financial reporting risks. All of these categories entail risks of violating the Sharīʿah and, of course, other risks as well.

With regard to the relationship between Sharīʿah audit and Sharīʿah risk management, many modern approaches to internal audit are risk-based. It represents a set of procedures

followed by the Internal Audit Department to direct audit efforts towards the riskiest areas of the organisation, whether at the level of work centers such as departments, divisions and subsidiaries or at the level of activities within individual work centers. The same applies to risk-based Sharī'ah audit, as it is a methodology that links Sharī'ah audit to the comprehensive framework of Sharī'ah risk management in the organisation to provide a guarantee to the BOD that Sharī'ah risk management processes are being effectively managed.

The extent to which the COSO methodology can be applied to internal Sharī'ah audit

Before examining the possibility of applying the COSO methodology to the internal Sharī'ah audit function, it is worth noting that although its developers assert that it represents a step forward for effective auditing, they have not claimed it to be the last word in this discipline or that it stands in no need of further amendments. It should also be noted that the framework was developed in response to the huge changes in the landscape of institutional operations, which have necessitated the development of a comprehensive and forward-looking methodology that is able to address these new challenges. As such, applying the COSO methodology to the internal Sharī'ah audit process is, in our view, not only possible but desirable.

To illustrate, in the modern era, early attempts at adopting the best practices of conventional works appeared in the contemporary Muslim scholars' efforts to harmonise Islamic law with conventional law. The efforts of Al-Sanhuri (1952), Al-Zarqā (2021) and others were considered among the most advanced examples. However, as far as internal control is concerned, AAOIFI has responded to the existing approaches to governance and internal control in international financial practices. The recent call to adopt COSO in Sharī'ah internal control is a clear endorsement of such a move (AAOIFI, 2019). Besides AAOIFI, the IFSB adopted the same approach with regard to benefitting from best practices in coming up with their standards. This approach was explicitly mentioned in the objectives of the IFSB, in which it is stated: "The work of the IFSB complements that of the Basel Committee on Banking Supervision, International Organisation of Securities Commissions and the International Association of Insurance Supervisors" (IFSB, 2020). With regard to local initiatives, BNM has made an advanced effort in this respect. The establishment of "The Law Harmonisation Committee" is considered part of Malaysia's continuous efforts to strengthen the legal system and infrastructure to cater for the growing development of Islamic finance. In the same way, BNM has issued its revised SGF for IFIs to accommodate the latest policy developments related to compliance, internal control and risk management (BNM, 2019).

These regulatory and supporting bodies, with the guidance of their renowned Sharī'ah committee members, see advanced practices related to internal control as a technical approach to ensuring quality and effectiveness and do not consider their adoption to be a violation of the rules of Sharī'ah. A fundamental principle of Sharī'ah is that anything related to means that leads to enhanced efficiency in discharging one's responsibility without contravening a clear Sharī'ah ruling is permissible. Likewise, custom and established practices are fundamental principles in Islamic law, comprising a class of evidence that is given consideration as long as it is not in conflict with the Sharī'ah. In support of this point, the Islamic Fiqh Academy and AAOIFI allow the employment of certain customs and practices initiated for unlawful purposes as long as the way they are used does not violate the Sharī'ah. The clearest example of this is the adoption of LIBOR (a reference price based on usury) as a reference price for measuring profits in IFIs. Similarly, the Sharī'ah Advisory Council (SAC) of BNM in its 210th meeting, dated 23 December 2020, ruled that it is permissible to adopt Risk-Free Rates (RFR) that depart from LIBOR but are based on

compounding methodology which applies the same approach of compounding interest. They justify the permissibility on the basis that "the compounding methodology is merely an arithmetic method in determining the term rate that does not affect compliance of the transactions with Sharīʿah requirements" (BNM, 2021).

Besides customs and practices, public interest (*maṣlaḥāh*), especially in its contemporary applications, requires the implementation of the best discoveries of management sciences, especially in light of the weakness of governance and audit in the practice of many IFIs. *Maṣlaḥāh* is given consideration by Sharīʿah; in fact, it is the essence of *maqāṣid al-Sharīʿah*. The Sharīʿah aims to realise the interests of humanity and repel harm from them. Furthermore, *maqāṣid al-Sharīʿah* recommends putting to good use the best achievements of the human mind in developing methods and tools for optimum performance. This *maqāṣidi* alignment is founded in texts of the Qur'ān recommending what is good and prohibiting what is evil regardless of its source. The Prophet's (SAW) ratification of some pre-Islamic practices such as forward sale (*salam*) is a clear example of such adoption. Although he (SAW) made some modifications related to specifying the volume, weight and delivery date of *salam*, he accepted it in principle (Bukhari, 1422H).

In addition to the *maqāṣidi* considerations, the COSO framework embodies a comprehensive approach that encompasses all aspects of internal control and integrates the institution's activities in carrying out the tasks of auditing and risk management and these aspects are crucial to the success of the internal Sharīʿah control. It also emphasises the overall approach of the institution in carrying out all the tasks and overlaps between the tasks of the institution. An example of this approach is risk management, which is considered an integral part of the decision-making process in all activities of existing IFIs. The framework eschews literal-minded formality in applying the principles of oversight. It goes beyond inflexible adherence to policies and procedures in favor of the auditors exercising discretionary diligence, provided they commit themselves to high professional competence and integrity. That is because an effective internal control system is not simply a matter of strict adherence to policies and procedures; rather, it goes beyond that to the exercise of judgement and discretion. That is a relative matter that requires competence on the part of those carrying out the work.

The framework also places the highest priority on risk management in that it makes it an integral part of the decision-making process in all of the institution's activities and it is considered crucial for achieving goals and improving performance. Risk management in IFIs is considered the cornerstone for ensuring effective management of the institutions' assets and general compliance with the Sharīʿah rules and principles. In fact, the COSO control framework provides an integrated, systematic presentation of internal control and it lays down steps that can be easily applied to the Sharīʿah audit of IFIs. It starts with the comprehensive elements of control and then frames them in organizing principles. It then adds 87 focus points, with the aim of making the work of the supervisors precise. For example, in the context of auditing the element of the "control environment", it addresses the necessity of manifesting the principle of commitment to integrity and ethical values in the institution. Then it mentions the focus points in auditing this principle. These include establishing the principle of the role model (setting the tone at the top), defining standards of behavior, evaluating compliance with the standards of behavior and addressing deviations in a timely manner.

Notwithstanding the above justification to consider the COSO internal control framework, it remains to warn that it should not be slavishly and uncritically followed. That is because COSO's internal control framework came in response to developments that had occurred in the system of governance, conditions of quality and technological progress. Although it is in principle applicable to all institutions, whether financial or economic or service providers, not all the details are binding on institutions that lack the complexities of modern organisations, or that have not undergone all the phases of their developments, or that have their own peculiarities.

Conclusion and recommendations

After examining the extent to which COSO can be incorporated in the Sharīʿah-compliance function of IFIs, the authors have arrived at a number of conclusions. In general, the research found that IFIs are required to have a solid SGF in order to strengthen their Sharīʿah-compliance mechanism and ensure that all relevant IFI regulations comply with Sharīʿah rules and principles. Effective implementation of the Sharīʿah-compliance function will further promote stakeholder confidence, as well as the integrity of the IFIs, by reducing Sharīʿah non-compliance risks. Besides that, Sharīʿah audit as an important part of governance represents one of the management functions aimed at ensuring the achievement of approved goals and reducing risks that an organisation may face. Likewise, internal Sharīʿah oversight is a crucial part of the governance of IFIs that aims to ensure that the transactions undertaken by the institution are in compliance with the provisions of Sharīʿah.

The adoption of the COSO methodology in the internal Sharīʿah audit process, as suggested by AAOIFI and deliberated in this research, is not only possible but desirable. This is because the existing frameworks of Sharīʿah supervision, whether AAOIFI's or the BNM's, though benefiting to some extent from the COSO framework, need to be further enhanced by widening the incorporation of the COSO methodology. In addition, the COSO framework places the highest priority on risk management in that it makes it an integral part of the decision-making process in all the institution's activities. This is in line with the basis of Islamic finance, which considers risk management as the cornerstone for ensuring end-to-end Sharīʿah compliance. As a result, incorporating the comprehensive COSO risk management structure within the Sharīʿah-compliance function will enhance IFIs' risk management and compliance.

The study also found that the COSO control framework provides an integrated, systematic presentation of internal control and that it lays down steps that can be easily applied to the Sharīʿah audit of IFIs. Indeed, its overall objective is to provide reasonable assurance regarding the achievement of the institution's goals at the following levels: the effectiveness and efficiency of operational processes, the reliability of financial reports and compliance with laws and regulations.

In addition, the study has shown that there is a need to conduct further research to compare the COSO framework with that of AAOIFI and BNM to examine whether there are any contradictions between them. Further research is also needed to better examine the components of the COSO framework and explore the ways that it could be integrated and harmonised within the Sharīʿah-compliance function of IFIs.

References

AAOIFI (2004), *Accounting, Auditing and Governance Standards for Islamic Financial Institutions (Arabic Version)*, Accounting and Auditing Organization for Islamic Financial Institutions, Manama.

AAOIFI (2007), *Sharīʿah Standards for Islamic Financial Institutions (Arabic Version)*, Accounting and Auditing Organization for Islamic Financial Institutions, Manama, Bahrain.

AAOIFI (2015), *Sharīʿah Standards for Islamic Financial Institutions (English Version)*, Accounting and Auditing Organization for Islamic Financial Institutions, Manama.

AAOIFI (2018), "Exposure draft of the governance standard for Islamic financial institutions: waqf governance", available at: http://aaoifi.com/wp-content/uploads/2019/03/Waqf-Governance-Exposure-Draft-v-8.4-Final-for-Publishing-.pdf (accessed 3 August 2020).

AAOIFI (2019), "Governance standard for Islamic financial institutions (GSIFI) No. 9 'Sharīʿah compliance function'", available at: http://aaoifi.com/gsifi-9-Sharīʿah-compliance-function/?lang=en (accessed 3 May 2019).

Abd Rahman, N., Mastuki, N., Kasim, N. and Osman, M.R. (2018), "Risk based internal Sharīʿah audit practices in the Islamic bank", *The Journal of Social Sciences Research*, Vol. 5, pp. 954-961, Special Issue.

Aden Abdi, A. (2017), "Applicability of COSO internal control framework on Islamic financial transactions. Case study: *murabaha* transaction", Master's thesis, The International Centre for Education in Islamic Finance (INCEIF), Kuala Lumpur.

Alamgir, M. (2007), "Corporate governance: a risk perspective", *Paper Presented at Conference on Corporate Governance and Reform: Paving the Way to Financial Stability and Development*, Egyptian Banking Institute, Cairo.

Algabry, L., Alhabshi, S.M., Soualhi, Y. and Alaeddin, O. (2020), "Conceptual framework of internal Sharīʿah audit effectiveness factors in Islamic banks", *ISRA International Journal of Islamic Finance*, Vol. 12 No. 2, pp. 171-193.

Al-Obaid, Y.J. (2017), "Legislative, financial and administrative framework", *Paper Presented at the Governance Conference in the State of Kuwait*, 10–11 October.

Al-Sanhuri, A.al-R. (1952), "Al-Wasit li Sharh al-Qanun al-Madani al-Jadid", Middle Commentary on the New Civil Code, 10 parts in 12 volumes, Cairo (1952–1970).

Al-Zarqā, M.A. (2021), *An Introduction to the General Theory of Obligations in Islamic Jurisprudence: A Thorough Formulation of the Theory's Texts*, (International Shari'ah Research Academy for Islamic Finance, Trans.), ISRA RMC, Kuala Lumpur.

BNM (2019), "Shariah governance", available at: https://www.bnm.gov.my/documents/20124/761679/Shariah+Governance+Policy+Document+2019.pdf (accessed 11 April 2022).

BNM (2021), "Ruling of the bank's Shariah Advisory Council on the adoption of risk-free rate", available at: https://www.bnm.gov.my/-/sac-bnm-210th-meeting (accessed 11 April 2022).

Briciu, S., Dănescu, A.C., Dănescu, T. and Prozan, M. (2014), "A comparative study of well-established internal control models", *Procedia Economics and Finance*, Vol. 15, pp. 1015-1020, doi: 10.1016/S2212-5671(14)00662-5.

Bukhari, M.B.I. (1422H), *Sahih Al-Bukhari*, Dar Tauq al-Nijat, Beirut.

CIBAFI (2017), "CIBAFI comments on the AAOIFI exposure draft on governance standard No. 9 Sharīʿah compliance function", The General Council for Islamic Banks and Financial Institutions, available at: https://cibafi.org/Files/L1/Content/CI1661-CIBAFICommentsontheAAOIFIEDonStandardNo.9_.pdf (accessed 13 August 2020).

COSO (2013), "Internal control, integrated framework: executive summary", The Committee of Sponsoring Organizations of the Treadway Commission, available at: https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf (accessed 8 April 2019).

COSO (2017), "Enterprise risk management integrating with strategy and performance", available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (accessed 10 April 2019).

Deloitte (2014), "Implementing the updated 2013 COSO framework: takeaways for banking and capital markets firms", available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-cosoframework2013-032414.pdf (accessed 30 April 2022).

Hidayah, N. (2014), "Religious Compliance in Islamic Financial Institutions", Doctoral Dissertation, Aston University.

IFSB (2009), *Guiding Principles on Shari'ah Governance Systems for Institutions Offering Islamic Financial Services*, Islamic Financial Services Board, Kuala Lumpur.

IFSB (2020), "Background", available at: https://www.ifsb.org/background.php (accessed 11 April 2022).

IIA (2017), *International Standards for the Professional Practice of Internal Auditing*, The Institute of Internal Auditors Malaysia, Kuala Lumpur.

Lawson, B.P., Muriel, L. and Sanders, P.R. (2017), "A survey on firms' implementation of COSO's 2013 internal control–integrated framework", *Research in Accounting Regulation*, Vol. 29 No. 1, pp. 30-43.

Mashal, A. (2015), "The integrated framework for the governance of the Islamic financial industry", *Paper Presented at the 14th AAOIFI Conference on Sharīʿah Boards for Islamic Financial Institutions*, Bahrain.

National Bank of Egypt (2003), "The method for exercising good corporate governance in companies: corporate governance", *Economic Bulletin*, Vol. 56 No. 2, p. 7.

Rezaee, Z. (1995), "What the COSO report means for internal auditors", *Managerial Auditing Journal*, Vol. 10 No. 6, pp. 5-9.

Shafii, Z. and Salleh, S. (2010), "Enhancing governance, accountability and transparency in Islamic financial institutions: an examination into the audit of Shari'a internal control system", *Malaysian Accounting Review*, Vol. 9 No. 2, pp. 23-42.

Shura (2019), "Final statement and recommendations of the 8th Shura Sharia Audit Conference", 6–8 October 2019, Grand Millennium Hotel, Muscat, Oman.

Udeh, I. (2019), "Observed effectiveness of the COSO 2013 framework", *Journal of Accounting and Organizational Change*, Vol. 16 No. 1, pp. 31-45.

Uwadiae, O. (2015), "COSO – an approach to internal control framework", available at: https://www2.deloitte.com/ng/en/pages/audit/articles/financial-reporting/coso-an-approach-to-internal-control-framework.html (accessed 6 April 2019).

Yazkhiruni, Y., Nurmazilah, M. and Haslida, A.H. (2018), "A review of Sharīʿah auditing practices in ensuring governance in Islamic financial institution (IFIs) – a preliminary study", *Advances in Social Sciences Research Journal*, Vol. 5 No. 7, pp. 196-210.

Zakaria, N., Mohd Ariffin, N. and Zainal, H. (2019), "Internal Sharīʿah audit effectiveness and its determinants: case of Islamic financial institutions in Malaysia", *Kyoto Bulletin of Islamic Area Studies*, Vol. 12 No. 1, pp. 8-28.

About the authors

Said Bouheraoua, PhD, is currently a Senior Researcher and Director of Research Development and Innovation Department at ISRA Research Management Centre (ISRA RMC) and a lecturer at INCEIF University, Kuala Lumpur, Malaysia.

Fares Djafri, PhD, is an Islamic finance Researcher at ISRA RMC, INCEIF University, Kuala Lumpur, Malaysia. He is an AAOIFI-Certified Shariah Advisor and Auditor (CSAA). He has published many chapters in books and several articles in the area of Islamic finance, takāful, Islamic banking regulations, and Sharīʿah governance. Fares Djafri is the corresponding author and can be contacted at: fares-isra@inceif.org, djafrifares@gmail.com