Getting Ahead With Fresh Perspectives

ICFR Benchmark Survey 2020

Grant Thornton

Contents

Grant Thornton is a market leader in providing ICFR services to many well-known entities in Abu Dhabi.

Our dominant market position is not by chance, rather by tailoring our Methodology to meet the business needs of our clients, engaging the right delivery team and providing fresh insights

Mohamed Elewa
Advisory Partner

Foreword

Grant Thornton is pleased to present our first annual Internal Control over Financial Reporting (ICFR) Benchmarking survey regarding compliance with Abu Dhabi Accountability Authority (ADAA) Resolution Number 1.

The Resolution requires government entities in Abu Dhabi to implement an ICFR framework which is to be tested by the external auditor.

We aim for our benchmark data to provide ICFR leaders with an overview of emerging practices in the market and the challenges faced in implementing an integrated and effective framework, along with key trends in managing and improving the efficiency, effectiveness and overall integration of the internal control framework.

The survey also aims to address some of the questions that are frequently asked by ICFR leaders and teams in the course of implementing and managing their ICFR frameworks. Our survey has covered a number of diverse sectors as well as relatively newly-established entities.

We have received 32 responses for this year's benchmarking survey with the majority of the responding entities reporting that they have recently implemented an ICFR program, while almost one quarter of entities reported that they are currently in the process of implementing an ICFR framework.

We would be pleased to discuss the results of our benchmark survey with you, share our knowledge and experience that can assist you in documenting and developing a process for evaluating internal controls in your entity.

Samer Hijazi

Partner, Head of Abu Dhabi Office
Grant Thornton UAE

T +971 2 666 9750
M +971 56 742 3109
samer.hijazi@ae.gt.com

Mohamed Elewa

Advisory Partner
Grant Thornton UAE

T +971 2 666 9750
M +971 56 975 8454
mohamed.elewa@ae.gt.com

In which year did your entity implement the requirements of ADAA Resolution No. 1 with respect to ICFR frameworks?

2019	41%
2018	31%
2017	6%
In-progress	22%

Have you attended the ICFR/COSO training sessions hosted by Grant Thornton and presented by Trent Gazzaway, National Managing Partner of Audit Quality and Innovation for Grant Thornton USA?

February 2020 session	66%
June 2018 session	9%
Have not attended	16%
Attended both sessions	9%

Which ICFR Framework Should I Adopt?

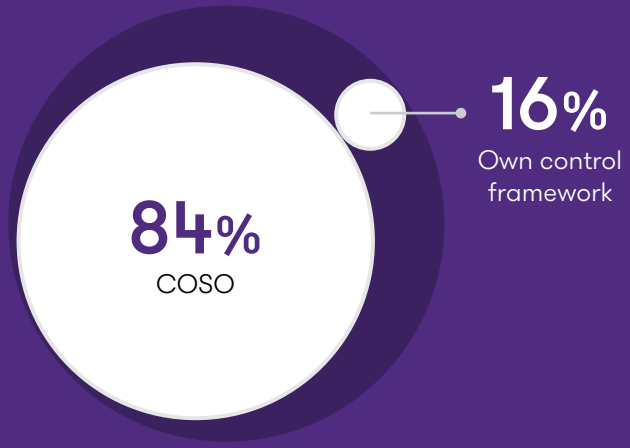
Entities adopt an integrated framework to not only cover the potential Financial Reporting Risks, but also to cover any operational and compliance Risks as well.

The main purpose of an integrated framework is to help management to better control the organisation's risks, create business value and to provide the C- Suite, Senior Leadership, Audit Committee and the Board of Directors with an ability to oversee how the implemented internal control is performing as well as to provide superior business MI and KPI reporting.

84% of the surveyed entities in Abu Dhabi selected the COSO framework for their ICFR program, 22% of which are still in the process of implementing ADAA Resolution No. 1.

Entities in Abu Dhabi are free to select the framework that meets their needs and achieves the desired objective of having an effective ICFR program in place. Interestingly, we noted that 16% of the surveyed entities adopted their own internal control framework. It is worth mentioning that 3 out of the 32 surveyed entities are not actually subject to ADAA Resolution No. 1 but still chose to follow its requirements.

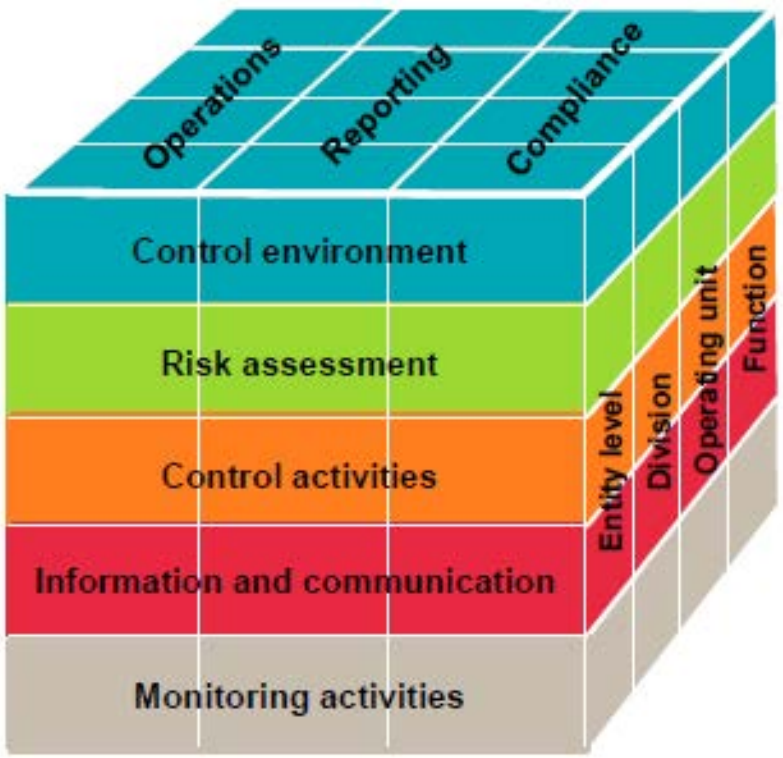
Which ICFR framework have you chosen to adopt in your organisation?



Selecting a suitable and/or recognised internal control framework is key to ensuring the successful implementation of an entity's ICFR program.

One of the most common frameworks adopted for the establishment and assessment of internal controls is the COSO framework (Committee of Sponsoring Organizations of the Treadway Commission) with its 5 key components as shown below in the 'COSO cube'.

COSO is one of the most commonly used and recognised frameworks around the world, and has been adopted by many leading international organisations and government entities.



While entities are free to build their own framework, in our view, implementing a globally recognised framework such as COSO can be more efficient and cost-effective, especially for those entities with limited resources available to dedicate to such a project.

ICFR Framework
Design & Implement

How did your entity design and implement the ICFR Framework?

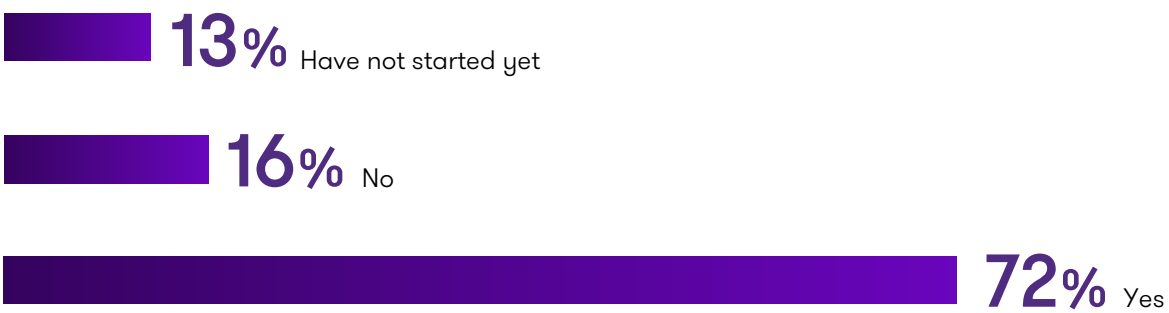
of the surveyed entities hired a third-party consultant to help with the design and implementation of their ICFR framework

Around 22% of the respondents decided to design and implement the ICFR framework in-house. The majority of the respondents reported that their entity preferred to engage with third-party consultants to design and implement the ICFR framework for various reasons, including lack of in-house resources/expertise and also to take advantage of the opportunity to draw upon a broader business perspective, access to market leading practices and benchmarking information.

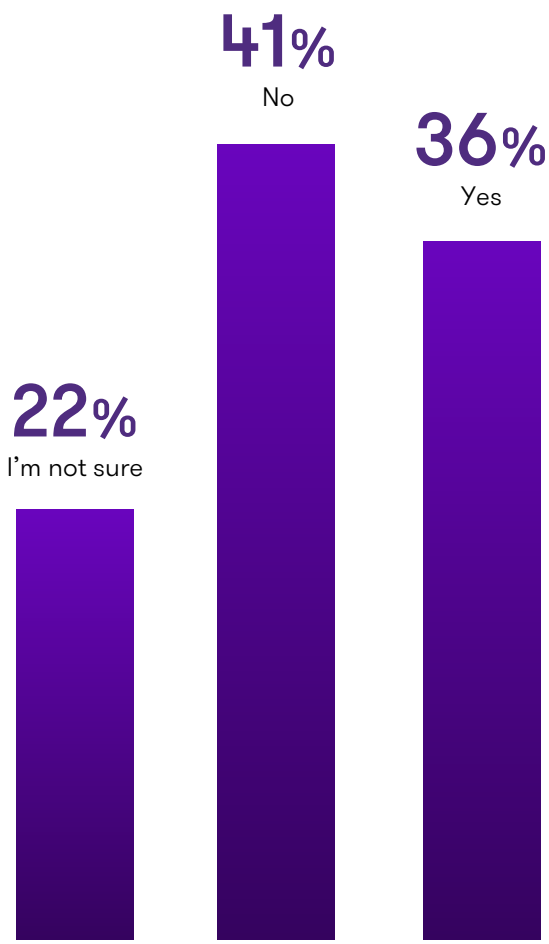
Does your entity have a defined process for evaluating the ICFR framework, at least on an annual basis?

Leading practice dictates that a defined process should be in place to regularly evaluate and update the ICFR framework including the quality of processes, scope and risk assessments, control design, and remediation plan.

The majority of the surveyed respondents confirmed that their entity has an annual process in place to update the ICFR program.



Do you regularly update your ICFR framework to respond to changes in the business regulatory requirements?



As a matter of best practice, any system of internal control needs to be agile in adapting to the new and rapidly-changing business environment, greater use and dependence on technology, increase in regulatory requirements and scrutiny, globalisation, and other challenges as they arise, e.g. a global pandemic.

Without having a robust process in place to respond to market changes and to reflect new regulations and laws, the internal control system may not be as effective nor able to achieve its objectives.

While many of the respondents have a process in place to update their ICFR framework on an annual basis, more than half of the respondents either do not update their ICFR periodically or are not sure whether it is actually updated to reflect emerging business and regulatory changes as they take place.

A Dedicated Team for ICFR

An internal control framework can only be as good as the people who are managing and overseeing its effectiveness on a daily basis.

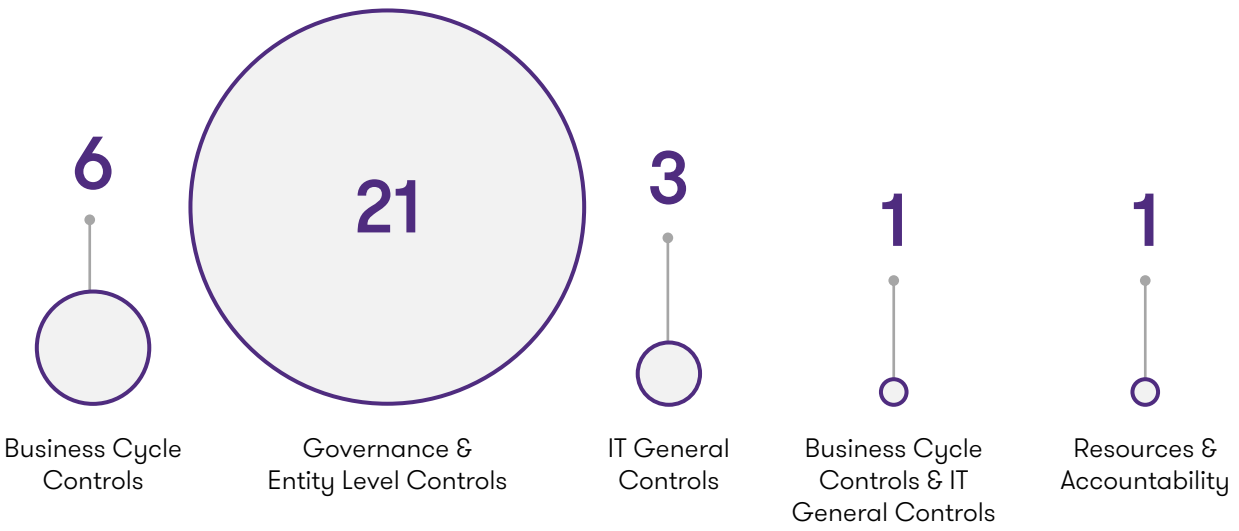
Internal control is impacted by the internal personnel, including the Board of Directors, or an equivalent oversight body for some of our surveyed entities and its committees, management and personnel, business enabling functions, and internal auditors. These functions are all collectively contributing in order to provide reasonable assurance to ensure specified objectives are achieved.

66% of the respondents indicated that they have designated staff, or a function with defined roles and responsibilities, to manage their ICFR program.

To gain an overview of the challenges faced by the market, we explored the main pain points of our participants in maintaining a functioning ICFR framework.

In your opinion, which area carries the highest level of risk and challenges when maintaining an ICFR framework?

The graph below shows the highest risk areas as reported by the number of entities. Governance and entity level controls are, by far, perceived to be the most challenging areas. This may not be surprising given that corporate governance in the GCC, in general, still needs further time to mature.



28% of the respondents noted that their entity does not have a designated team to oversee the ICFR program.

Several participants also responded that they do not have clarity on who should be managing the ICFR program internally.

Furthermore, 3 of these participants also reported that their entity received a qualified opinion from their External Auditor on their ICFR - while there is insufficient data to conclude whether there is a link between the absence of a dedicated ICFR team and the likelihood of receiving a qualified opinion, in our view, having a designated team to oversee the ICFR program with clear roles and responsibilities is likely to reduce the risk of a qualified opinion.

Did your entity dedicate designated staff with defined roles and responsibilities to manage and oversee the ICFR program?

25%
have a designated function & help of a Service Provider

41%
have a designated function to oversee ICFR Program

28%
do not have a designated staff / function, as it is not clear who should manage and oversee ICFR

6%
have not started yet

The 3 Lines of Defense and ICFR

One of the most common questions we are asked is "what is the role of the "Three Lines of Defense" in maintaining an effective ICFR framework, such that all of the components of internal control are present and functioning in an integrated manner?"

Firstly, let's take a closer look at the roles and responsibility of each line of defense.

1st Line of Defense

Under the first line of defense, operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.

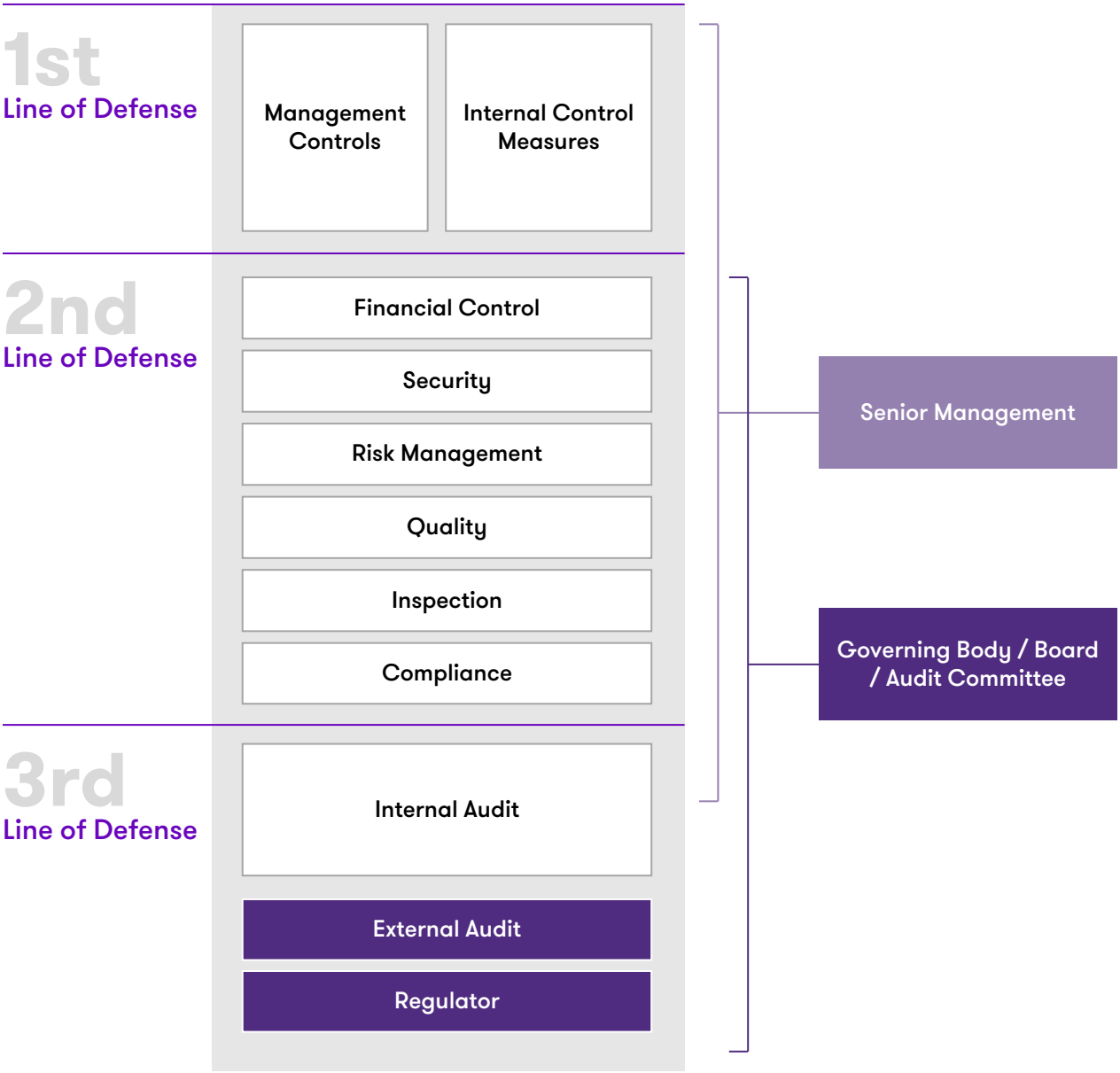
2nd Line of Defense

The second line of defense consists of activities covered by several components of internal governance (compliance, risk management, quality, IT and other control departments). This line of defense monitors and facilitates the implementation of effective risk management practices by operational management, and assists the risk owners in reporting adequate risk-related information across the organisation.

3rd Line of Defense

Internal audit forms the organisation's third line of defense. An independent internal audit function will, through a risk-based approach to its work, provide assurance to the organisation's board of directors and senior management. This assurance will cover how effectively the organisation assesses and manages its risks, and will include assurance on the effectiveness of the first and second lines of defense.

The third line of defense encompasses all elements of an institution's risk management framework (from risk identification, risk assessment and response, to communication of risk related information) as well as all categories of organisational objectives: strategic, ethical, operational, reporting and compliance.



The role of the three lines of defense

Internal audit is uniquely positioned within the organisation to provide global assurance to the audit committee and senior management on the effectiveness of internal governance and risk processes.

It is also well-placed to fulfil an advisory role on the coordination of assurance, effective ways of improving existing processes, and assisting management in implementing recommended improvements.

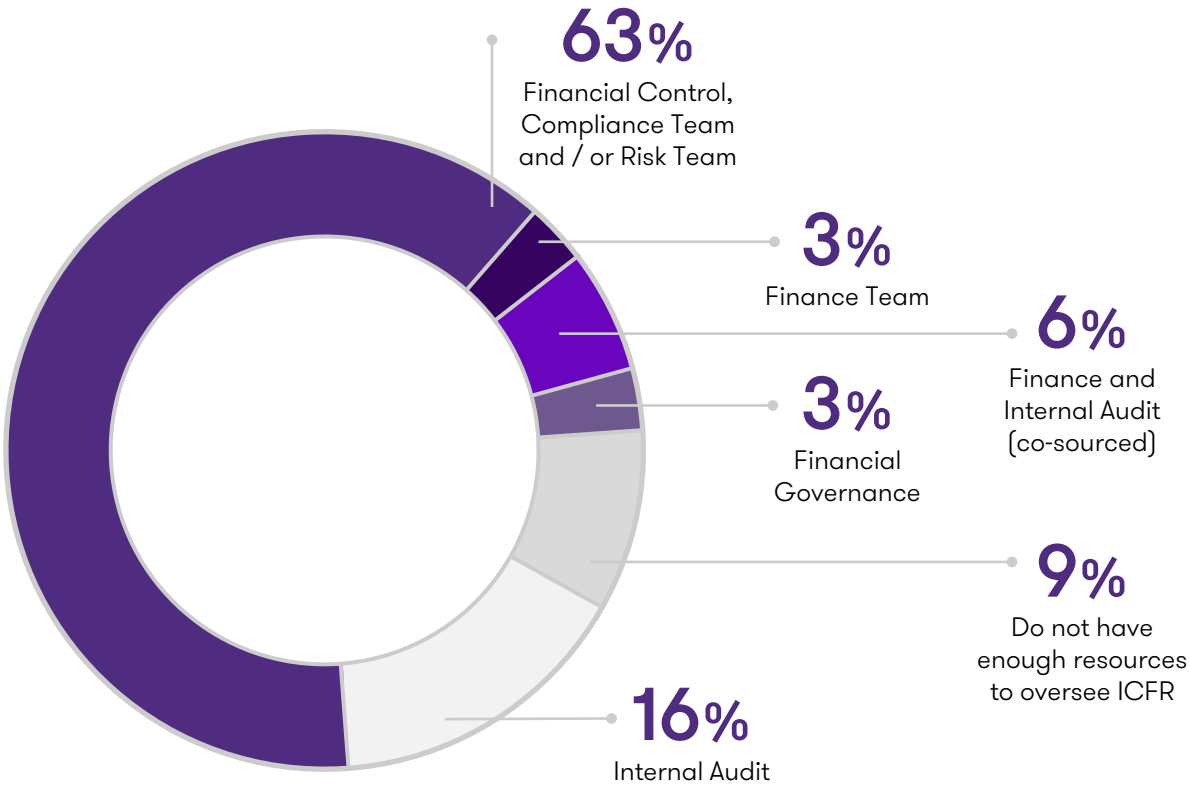
In such a framework, internal audit is the cornerstone of an organisation's corporate governance.

The use of the 3 lines of defense to understand the systematic role of internal control and risk management should not be regarded as an automatic guarantee of success. All 3 lines need to work effectively with one another as well as with the audit committee in order to create the right conditions.

The majority of the surveyed entities appear to have their ICFR framework managed within the Second Line of Defense. However, 16% of the respondents have also asked their internal auditors to manage their ICFR program, despite the conflicts that may arise.

Due to lack of resources, some of the surveyed entities have not assigned the responsibility for managing ICFR to any function within their entity, which indicates a lack of clear ownership of the ICFR.

Which part of your entity manages the ICFR?



Management owns the processes of identifying, managing and monitoring overall risks and internal controls, setting the tone at the top, and fostering a risk-aware culture. Studies have shown that strong risk management and systems of internal control have a positive impact on long-term business performance and earnings potential.

In our view, establishing a governance structure through the use of a well-defined and coordinated integrated risk and control model is the cornerstone of a strong risk management and ICFR framework. Organisations must define clear ownership and accountability for risk management and internal control activities to enable effective coordination, communication and reporting.

When it comes to an integrated risk and control model, one size does not fit all. Many factors come into play, including industry, size, location, regulatory requirements, and the risk culture. Even though each organisation needs to design and implement an integrated risk and control model that aligns with its strategies and governance structure, some elements are common among all companies.

Internal Control Deficiency Evaluation

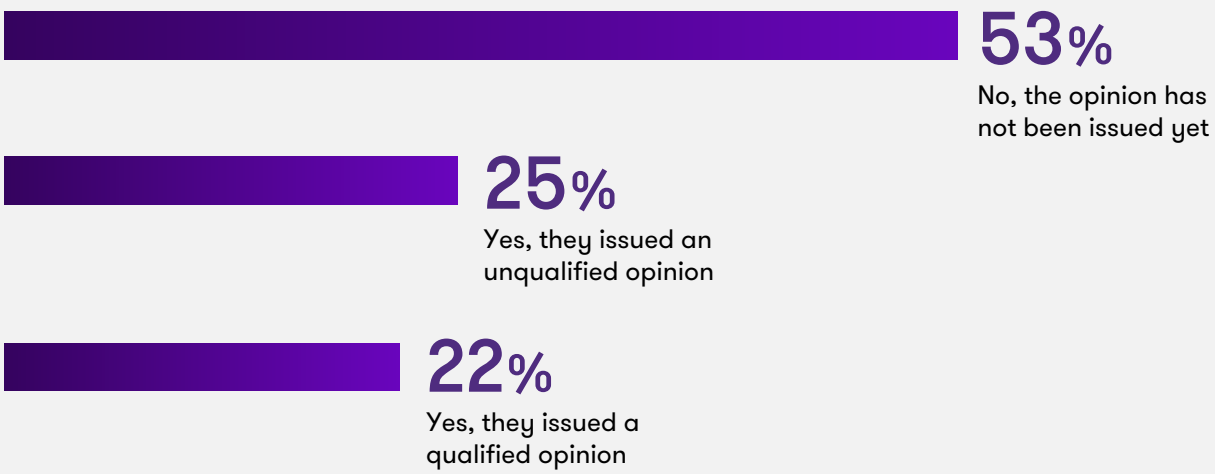
The external auditing body must evaluate the severity of each control deficiency and determine whether the deficiencies, individually or in combination, are considered material weaknesses as of the date of management's assessment.

The severity of any deficiency depends on 2 factors:

1. Whether there is a reasonable possibility that the entity's controls will fail to prevent or detect a misstatement of an account balance or disclosure

2. The magnitude of a potential misstatement resulting from the deficiency or deficiencies.

Has your external auditor issued a separate opinion on your ICFR?



The severity of a deficiency does not depend on whether a misstatement has actually occurred, but rather on whether there is a reasonable possibility that the entity's controls will not prevent or detect such misstatement in a timely manner.

As of April 2020, when this survey was circulated, the majority of respondents indicated that they had not yet received a separate opinion from their external auditor on the effectiveness of their entity's ICFR. However, 22% reported receiving a qualified opinion on the effectiveness of their entity's ICFR.

We recommend all entities to have an internal control deficiency evaluation process in place to review each deficiency noted and evaluate whether a control deficiency presents a reasonable possibility of misstatement, taking into consideration both qualitative factors (i.e. fraud) and quantitative factors (i.e. financial impact). This is to manage the risk of receiving a qualified opinion from the external auditor in the year end.

More than half of the responses received indicate that the Audit Committee evaluates control deficiencies, and very few surveyed entities appear to have a Disclosure Committee/ICFR Steering Committee in place to assess the impact of Control Deficiencies.

As leading practice, the initial discussion of control deficiencies should start at the process/control owner level for severity evaluation, then all deficiencies should be compiled and presented to the Management/Senior Leadership to determine the deficiency impact and required disclosures, if any , along with the Disclosure Committee/ICFR Steering Committee, to be finally presented to the Audit Committee to review management's decision on deficiency severity and disclosure needed.

How are the Internal Control Deficiencies evaluated at your Entity?

3%
Disclosure Committee / ICFR Steering Committee (or equivalent) evaluates all of the Internal Control Deficiencies

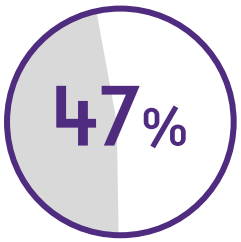
13%
We do not have any committees, so it is left up to management to assesses the impact on the financial statements

63%
Audit Committee evaluates all of the Internal Control Deficiencies

22%
I'm not sure

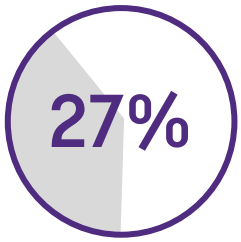
Third Party Service Providers

Do you have any outsourced systems and / or business processes in your entity?



of surveyed entities have outsourced systems and/or business processes to third-party service providers

Do you obtain an SOC report* for the outsourced systems and / or business processes in your entity?



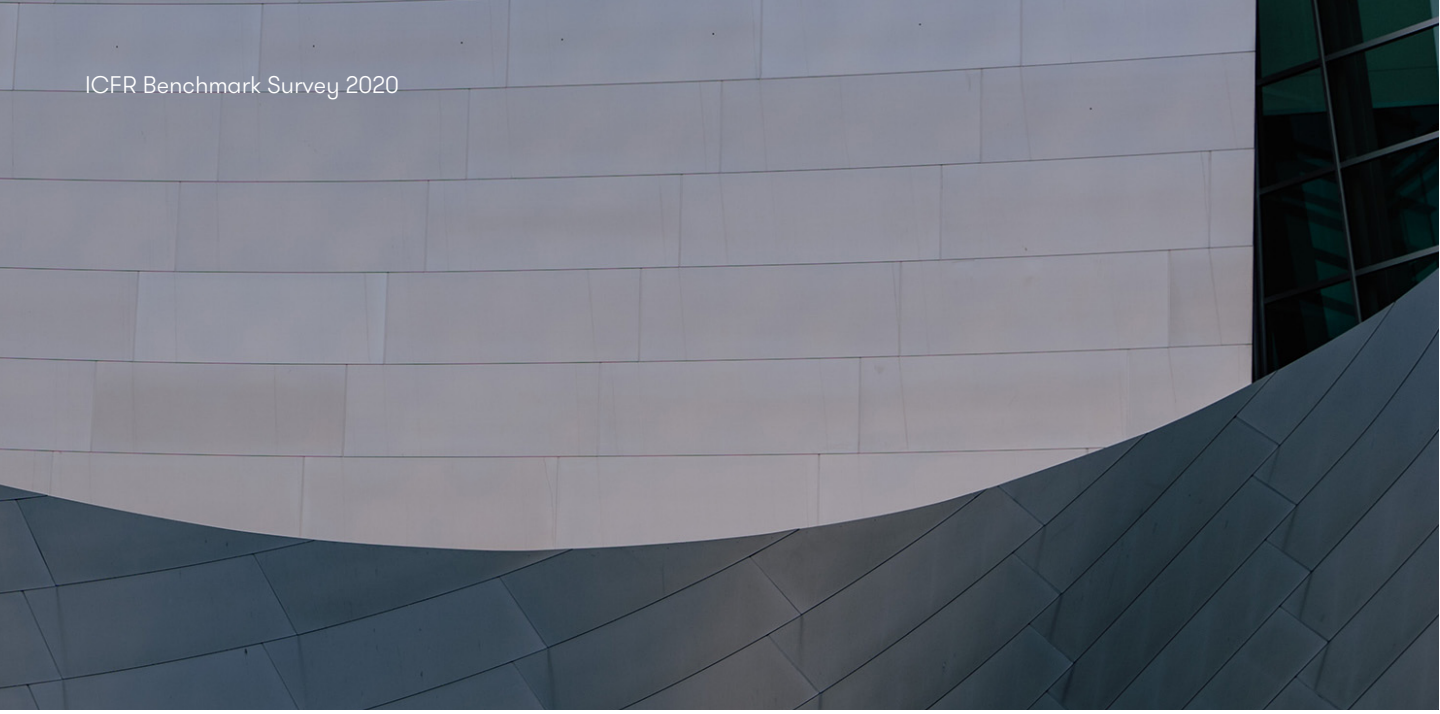
Obtain an SOC report for the outsourced services

When outsourced service providers perform controls on behalf of the entity, the management still retains responsibility for those controls performed on their behalf or performed under the direction of management.

In such cases, the entity should obtain a SOC report* on an annual basis, for the outsourced services that affect their ICFR to evaluate the management of risks associated with the use of third-party providers.

Interestingly, only 27% of surveyed entities obtain a SOC report and 40% are not sure if they obtain such report.

* An SOC Report (System and Organization Controls Report) is a report on Controls at a Service Organization which are relevant to user entities' internal control over financial reporting.

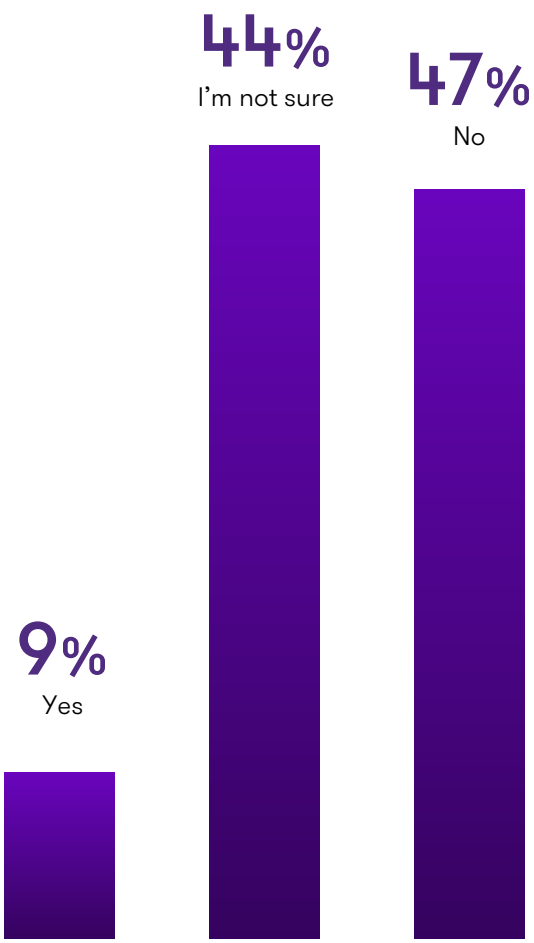


To gain a better understanding of market views of the ultimate responsibility for the work performed by the third-party services providers, we also asked the participants if they agree with the following statement:

> "The third-party service provider is solely responsible for having an effective internal control environment with respect to our outsourced systems and/or business processes. Provided we obtain a SOC report for the outsourced systems and/or business processes on a regular basis from the service provider then we have fully discharged our responsibility".

Clearly, a greater understanding of the role and relevance of SOC reports to the ICFR framework still needs to be developed in the market.

The results of responses received are illustrated below:

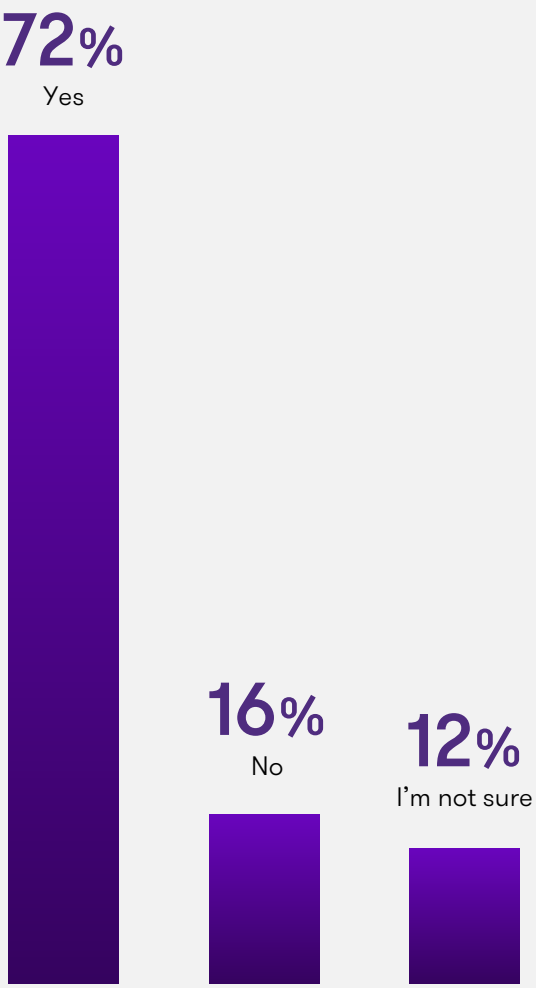


System Access Control

One of the primary concepts of internal control is to maintain segregation of duties to mitigate the fraud and error risks or at least reduce such risks to a manageable level.

In many instances, the finance team may be understaffed which naturally leads to shared responsibilities of key processes among the finance team.

Do the system access controls within your entity comply with leading practices of segregations of duties?



A few of the entities reported that they are closely monitoring material entries, so they are at least aware of all cases where adequate segregation of duties cannot be maintained. These entities keep a record of such cases, without escalating to Senior Management the fact that they are short of resources.

The majority of the surveyed entities indicated that their system access controls are in compliance with leading practices of dispersing compatible duties, however, in our experience, we noticed in the past few years a lack of segregation of duties at some entities, mainly due to a lack of resources.

Use of Spreadsheets

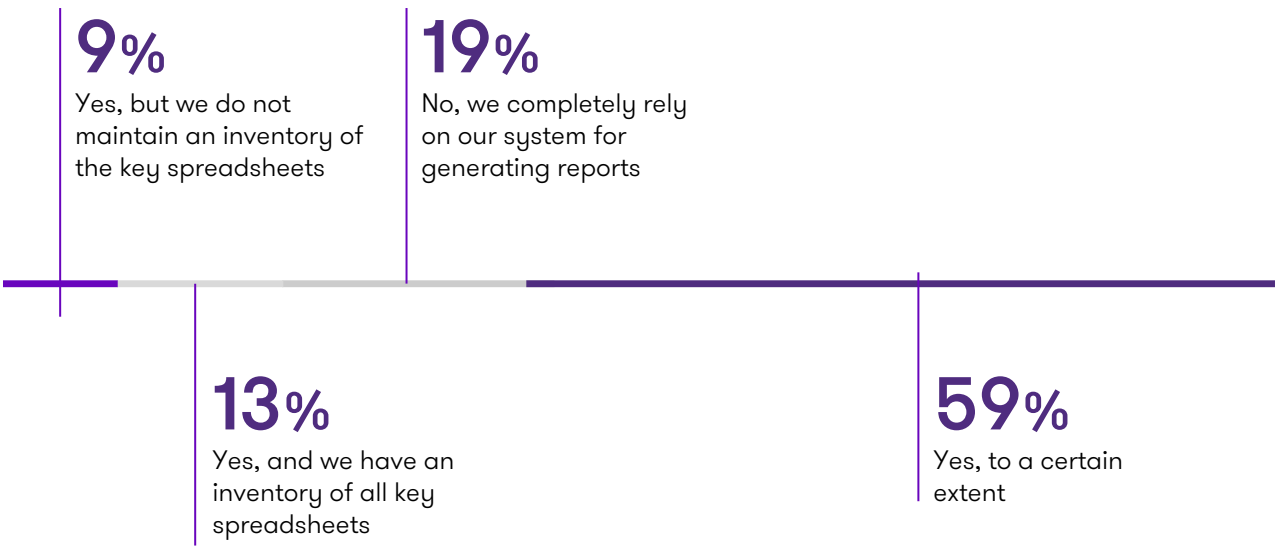
Spreadsheets are widely used for business-critical reporting, consolidation, computation of critical and material journal entries and corporate financial reporting.

A specific concern over the use of spreadsheets is the testing and protection of such spreadsheets.

There has long been evidence that spreadsheet errors are widespread and can lead to material errors, if not detected on a timely basis.

In our experience, many entities rarely keep a list of key spreadsheets used, mandate that spreadsheets be regularly tested or ensure that they are password protected and key cells/ formulas locked.

Are spreadsheets widely used in your entity as part of your ICFR framework?



13% reported that they maintain an inventory of all key spreadsheets, which are all password protected, with locked key cells and regular testing of the formula logic.

The use of spreadsheets should be combined with the following:

1.
A defined control process with enough detail that users/ auditors can follow it to understand the process

2.
Input controls and process controls need to be defined (i.e. key cells are locked; sheets are password protected)

3.
Maintain a record of changes to the logic of a spreadsheet and authorise these changes

4.
Maintain a historic record of actual changes

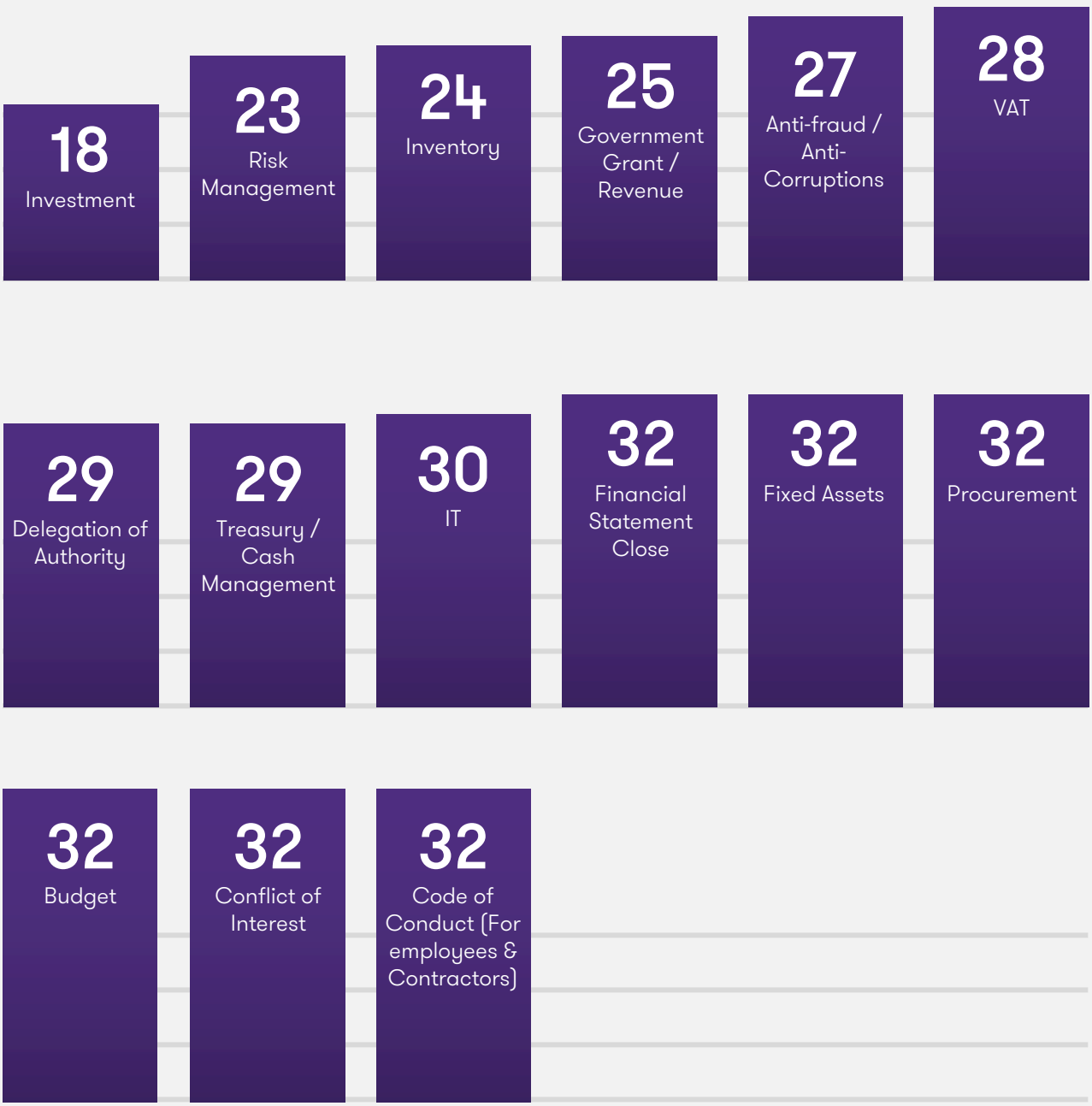
5.
Detailed review of the formula logic on regular basis

Policies and Procedures

Entities should maintain detailed processes, policies and procedures to provide a basis for how to get from their existing state to a desired target state and how risks are to be managed.

Entities need to outline current requirements, operations, interdependencies, risks and controls, this can help identify gaps and improvement opportunities. This also helps to shape direction, so an entity can move from a "check-the-box," compliance-first mindset to one that recognises risk management as a critical business discipline.

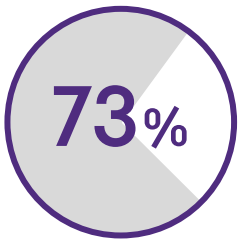
Below are the most common documented policies and procedures reported by the surveyed entities:



Moving Towards An Integrated Audit

Although the objectives of an audit of ICFR and an audit of financial statements are not the same, the auditor should plan and perform the integrated audit to achieve their respective objectives simultaneously.

Did your external auditor issue a separate opinion on your ICFR on the same date as the audit opinion on the financial statements?



Of surveyed entities received the external auditor report on ICFR on the same date as the external audit opinion on the financial statements

The auditor should design tests of controls to obtain sufficient appropriate audit evidence to support the auditor's opinion on ICFR as of the date specified in the management's assessment about ICFR and to obtain sufficient appropriate audit evidence to support the auditor's control risk assessments for purposes of the audit of financial statements.

The auditor should consider the effect of the financial statement auditing procedures results on the auditor's risk assessments and the necessary testing to conclude on the operating effectiveness of a control.

If, during the audit of ICFR, the auditor identifies a deficiency in ICFR, the auditor should determine the effect of the deficiency, if any, on the nature, timing, and extent of substantive procedures to be performed to reduce audit risk in the audit of the financial statements to an acceptably low level.

Because the audit of ICFR is integrated with the audit of the financial statements, when issuing separate reports on the entity's financial statements and on ICFR, the dates of the reports should be the same.

As such, while it is understandable that, due to the challenges of first-time implementation of the ICFR framework in Abu Dhabi, some entities received the opinion on the audit and the opinion on the ICFR on different dates.

In our view, best practice will move towards all auditors designing integrated audit approaches with the issuance of both opinions on the same date.

Remediating the findings

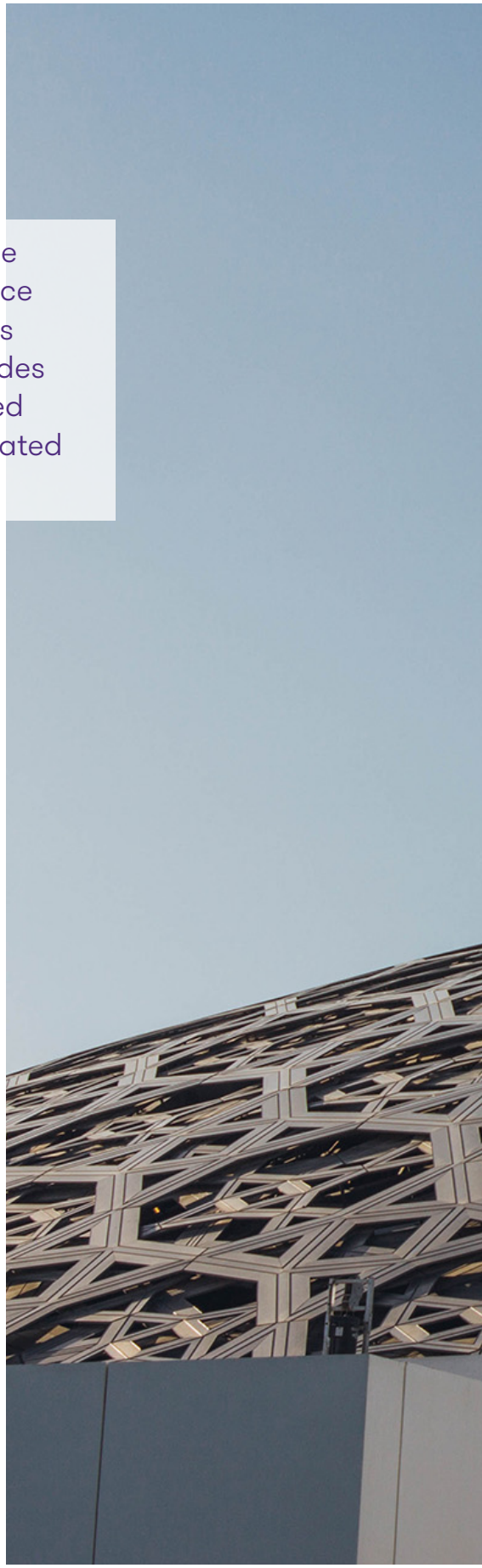
The auditor should communicate in writing to the management and those charged with governance significant deficiencies and material weaknesses identified during the integrated audit. This includes those that were remediated during the integrated audit and those that were previously communicated but have not yet been remediated.

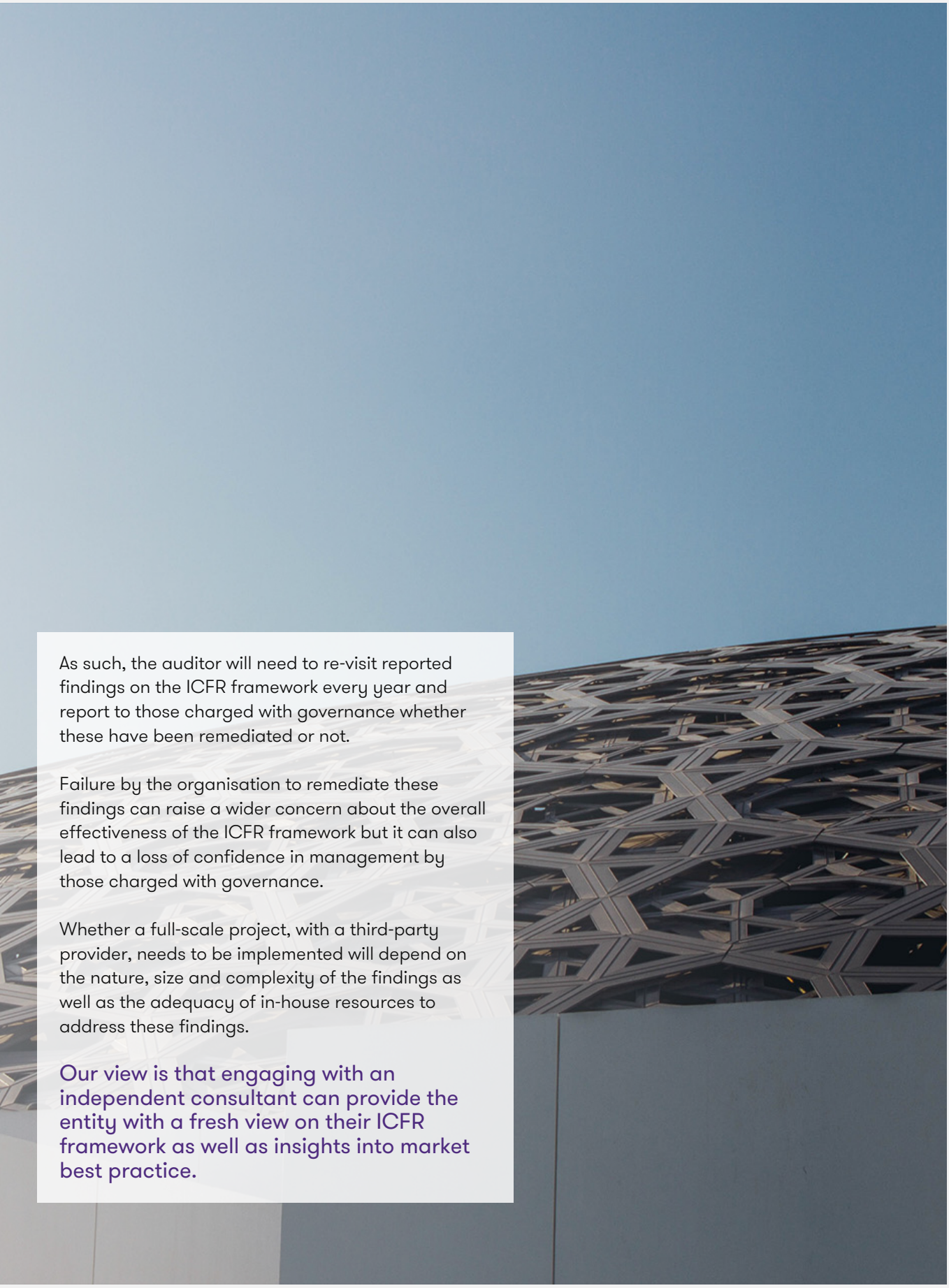
If you received a qualified opinion on your ICFR framework, are you taking any steps to remediate the findings reported?

43%
Yes, we have a project in place to address these findings

43%
Yes, we will be putting a project in place to address these findings

14%
No further action will be taken





As such, the auditor will need to re-visit reported findings on the ICFR framework every year and report to those charged with governance whether these have been remediated or not.

Failure by the organisation to remediate these findings can raise a wider concern about the overall effectiveness of the ICFR framework but it can also lead to a loss of confidence in management by those charged with governance.

Whether a full-scale project, with a third-party provider, needs to be implemented will depend on the nature, size and complexity of the findings as well as the adequacy of in-house resources to address these findings.

Our view is that engaging with an independent consultant can provide the entity with a fresh view on their ICFR framework as well as insights into market best practice.

The COVID-19 Impact

The impact of COVID-19 is rapidly evolving and has already resulted in major business disruptions, both locally and internationally.

While the repercussions of the COVID-19 outbreak may vary with respect to each sector, it is vital for all entities to re-evaluate their ICFR program to identify new risks, reassess existing controls and/or introduce new controls to manage emerging risks and monitor ICFR effectiveness (very often remotely).

41% of the surveyed entities responded that their ICFR program had not been affected by the COVID-19 global pandemic while more than half were still to carry out an assessment as to whether their ICFR program had been impacted.

The results of the COVID-19 outbreak will require a re-evaluation of the following considerations:

Control Environment

Management needs to pay attention to the evaluation and response to the new risks created by the COVID-19 outbreak as well as the impact of remote working arrangements:

Assessing operating effectiveness

Entities may consider reevaluating their monitoring activities to determine whether controls have become less effective or are no longer operating as designed and implemented. Existing monitoring activities may need to be modified to operate effectively in a remote working environment.

Financial reporting operating resiliency

Entities might also need to assess the business capability to prepare financial statements completely, accurately and on a timely basis. Pandemic-related risk indicators include subsidiary locations in lockdown, attrition or illness of qualified personnel, and facilities or financial reporting hubs functioning remotely or going offline.

The potential global and economic impacts of the COVID-19 continue to evolve rapidly, and entities should monitor the situation. Entities should remain focused, pay attention to changes in anticipation of their internal control re-evaluation.

Reach out:

Grant Thornton has a fully certified COSO Team to assist you with all your requirements. To discuss the results of the survey and how we can help, please contact:

Samer Hijazi

Partner, Head of Abu Dhabi Office
Grant Thornton UAE

T +971 2 666 9750
M +971 56 742 3109
samer.hijazi@ae.gt.com

Mohamed Elewa

Advisory Partner
Grant Thornton UAE

T +971 2 666 9750
M +971 56 975 8454
mohamed.elewa@ae.gt.com

Abu Dhabi

Al Kamala Tower
Office 1101, 11th Floor
Zayed the 1st Street
Abu Dhabi, UAE

T +971 2 666 9750
F +971 2 666 9816

Abu Dhabi

Office 3414, 34 Floor
Al Maqam Tower
ADGM Square
Al Maryah Island
Abu Dhabi, UAE

T +971 2 666 9750
F +971 2 666 9816

Dubai

Rolex Tower, 23 Floor
Sheikh Zayed Road
PO Box 1620
Dubai, UAE

T +971 4 388 9925
F +971 4 388 9915

Sharjah

Al Bakr Tower
Office 305
7/9 Al Khan Street
Sharjah, UAE

T +971 6 525 9691
F +971 6 525 9690