ACCA Think Ahead

Internal Audit FOUNDATION

ima The Association of Accountants and Financial Professionals in Business

INTERNAL CONTROL AND THE TRANSFORMATION OF ENTITIES

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants.

We are a thriving community of 233,000 members and 536,000 future members based in 178 countries and regions, who work across a wide range of sectors and industries. We uphold the highest professional and ethical values.

We offer everyone everywhere the opportunity to experience a rewarding career in accountancy, finance and management. Our qualifications and learning opportunities develop strategic business leaders, forward-thinking professionals, with the financial, business and digital expertise essential for the creation of sustainable organisations and flourishing societies.

Since 1904 being a force for public good has been embedded in our purpose. In December 2020, we made commitments to the UN Sustainable Development Goals, which we are measuring and will report on in our annual integrated report. We believe that accountancy is a cornerstone profession of society and is vital in helping economies, organisations and individuals grow and prosper. It does this by creating robust trusted financial and business management, combating corruption, ensuring organisations are managed ethically, driving sustainability, and providing rewarding career opportunities.

And through cutting edge research, we lead the profession by answering today's questions and preparing for the future. We are a not-for-profit organisation.

Find out more about us at www.accaglobal.com

About The Internal Audit Foundation and the Institute of Internal Auditors

The Internal Audit Foundation is an essential global resource for advancing the internal audit profession.

Foundation-funded research provides internal audit practitioners and their stakeholders with insight on emerging topics and promotes and advances the value of the internal audit profession globally. In addition, through its Academic Fund, the Foundation supports the profession's future by providing grants to students and educators who participate in The Institute of Internal Auditor's Internal Auditing Education Partnership Program.

For more information, visit www.theiia.org/Foundation

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 210,000 members from more than 170 countries and territories.

For more information, visit www.theiia.org

About IMA® Institute of Management Accountants

IMA® is one of the largest and most respected associations focused exclusively on advancing the management accounting profession.

Globally, IMA supports the profession through research, the CMA® (Certified Management Accountant) and CSCA® (Certified in Strategy and Competitive Analysis) programs, continuing education, networking, and advocacy of the highest ethical business practices. Twice named Professional Body of the Year by The Accountant/International Accounting Bulletin, IMA has a global network of about 140,000 members in 150 countries and 350 professional and student chapters. Headquartered in Montvale, N.J., USA, IMA provides localized services through its four global regions: The Americas, Asia/Pacific, Europe and Middle East/India.

For more information about IMA, please visit www.imanet.org

Copyright © July 2022 by the Association of Chartered Certified Accountants (ACCA), The Internal Audit Foundation (IAF) and The Institute of Management Accountants (IMA).

All rights reserved. Used with permission of ACCA, IAF and IMA. Contact insights@accaglobal.com for permission to reproduce, store or transmit, or to make other similar uses of this document.

INTERNAL CONTROL AND THE TRANSFORMATION OF ENTITIES

Internal control is one of the fundamental concepts used by entities to achieve important objectives, improve performance and build reputation, especially in disruptive and uncertain times. Internal control forms a core part of the activities of accountancy, finance and internal audit professionals, assisting them in ensuring that entities operate effectively. Yet the nature of the business model is changing for many. Transformation, including the adoption of digital enablers, is changing the way that processes are undertaken. Rapid response to changing customer and economic factors is a reality. In this report, we explore these and other emerging trends, their impact on internal control and the need for internal controls to be agile and future-ready to support business transformation and growth.

The research is based upon a series of roundtables and interviews with more than 80 finance and internal audit professionals from a range of entities worldwide. Roundtable feedback is anonymised; however, geographic location is often cited to help readers identify comments where differences in regulations or cultural norms may vary due to location. The roundtables were supported by a survey of ACCA, IIA and IMA members, which received more than 1,950 responses (an overview of the survey demographics can be found in the Appendix).

Foreword

Effective internal control is one of the essential enablers for entities to grow with confidence and integrity in a multi-stakeholder world filled with volatility, uncertainty, disruption, and complexity. Internal control goes beyond statutory compliance requirements; it helps entities build trust, confidence, and a positive reputation in achieving strategic business outcomes.

Accountancy, finance, and internal audit professionals, whatever their role, are fundamental players, together with others, in the control frameworks of their entities. In today's rapidly evolving environment entities face many challenges. They need to transform continually and rapidly to ensure that they address an operating environment that is increasingly complex. Entities are increasingly using technology and data. Data-driven insights are essential to enable management to react quickly and take decisions across an increasingly broad horizon. Stakeholders are seeking disclosures that cover not only financial objectives, but also those that address non-financial areas such as actions in relation to climate change and human capital. These changes bring into play a broader scope of business activities that require effective internal control. Stakeholders are seeking trust and confidence beyond financial reporting, for example, through environmental, social and governance-related disclosures. A breadth and depth of skill sets needed to embrace internal control across this broader set of objectives is now needed.

Effective internal control requires an appropriate combination of people, processes, technology, and data underpinned by an unwavering commitment to trust and ethics. For accountancy, finance and internal audit professionals it is important to have a detailed appreciation of the opportunities that technology can present; how these are translated into processes enacted and the optimised ways of working. Through professional qualifications and continuous learning, these professionals need to ensure that they can maintain relevance, enabling them to guide decision makers in addressing the broadening governance and control requirements. In this way accountancy, finance and internal audit professionals are ready and able to guide their entities and the stakeholders into a new era for internal control.

Helen Brand OBE
Chief Executive, ACCA

Anthony J. Pugliese, CIA, CPA, CGMA, CITP
IIA President and Chief Executive Officer, Internal Audit Foundation Board of Trustees

Jeffrey Thomson, CMA, CSCA, CAE
Chief Executive Officer and President, Institute of Management Accountants

Contents

Executive summary

Internal controls are fundamental to enabling entities to grow with confidence and integrity. Since the corporate challenges of the 1970s, regulators have focused on ensuring that appropriate controls are in place in entities where there is significant public interest. This combination of investor and regulatory requirements generates a need to invest in processes and controls.

The operating models of many entities have been undergoing change as the focus has shifted from competition based upon bespoke and tailored enterprise resource planning (ERP)-based models to those based upon insight and analysis of customer behaviour. The mantra of 'five years in five months' has reflected the acceleration of technology-enabled transformation of entities during the pandemic, and that trend is expected to continue to accelerate as they move into a new set of economic challenges.

How has internal control been impacted by these changes? Should entities seek to reappraise their frameworks and embrace the opportunities that these technological transformations offer? This is the focus of the present research.

Approximately 1,950 ACCA, Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA) members responded to a survey and more than 80 participated in a series of roundtables and interviews that were held across the globe.

The purpose of internal control was reinforced by these contributors (as explored in Chapter 1). There was strong alignment to The IIA's Three Lines Model demonstrating the interrelated governance roles of the board, management, and internal auditors to assure and achieve effective internal controls over financial – and more recently – sustainability reporting. Yet as entities undertake their transformational journeys, a key skill shortage among those enacting the internal controls was highlighted.

Transformation is clearly having an impact on internal controls. Chapter 2 explores several of these issues. It has changed the operating models of most entities, but the nature of the impact on the internal control environment has been varied, with clear regional differences in the range of positive and negative impacts on entities. What is clear from the survey responses is that internal control frameworks and processes need to be incorporated early on as part of business transformations or strategic initiatives to achieve increased growth and value for multiple stakeholders. It should not be forgotten that transformation has four aspects: people, process, technology, and data. This is true of the transformation of internal control, and it is important not to lose sight of all these components in this discussion.

Transformation is itself transforming. No longer is it driven just by large-scale projects, but the use of Cloud-based solutions and other approaches means that increasingly it is an iterative and agile process. Micro-services to address immediate opportunities and challenges are the order of the day. As a result, control frameworks need to flex and change. Yet there is an apparent reluctance relative to the new business environment, for example, moving toward agile internal control and risk management, continuous and real-time monitoring, and digitization and automated controls (including use of XBRL).

Chapter 3 explores these challenges and offers insights and observations on potential next steps for entities. There is a need to ensure that internal control and risk-management frameworks are agile and fit for purpose in a business environment that is increasingly expanding in scope (for example, the need to manage and account for sustainability issues) with rapidly evolving technologies such as Cloud computing, artificial intelligence, blockchain and process mining. The nature of rapid change requires adaptive and agile leadership and project focus (see sections 3.2 and 3.3). Internal control must be integral to these advancements. The application of technology is also evolving as entities embrace the 'fourth industrial revolution' and connected technologies. This transition has implications for skills and controls (see section 3.5).

It is a change not only in the nature of control but a shift from a more static view to one that focuses more on near-real-time data flows, continuous and automated. There is also recognition of shared objectives, such as those concerned with governance over the integrity of data, and alignment to a dynamic risk culture that reacts to rapidly evolving operating models (section 3.7). Those entities that succeed are likely to be those that embrace the use of data, innovation and agility.

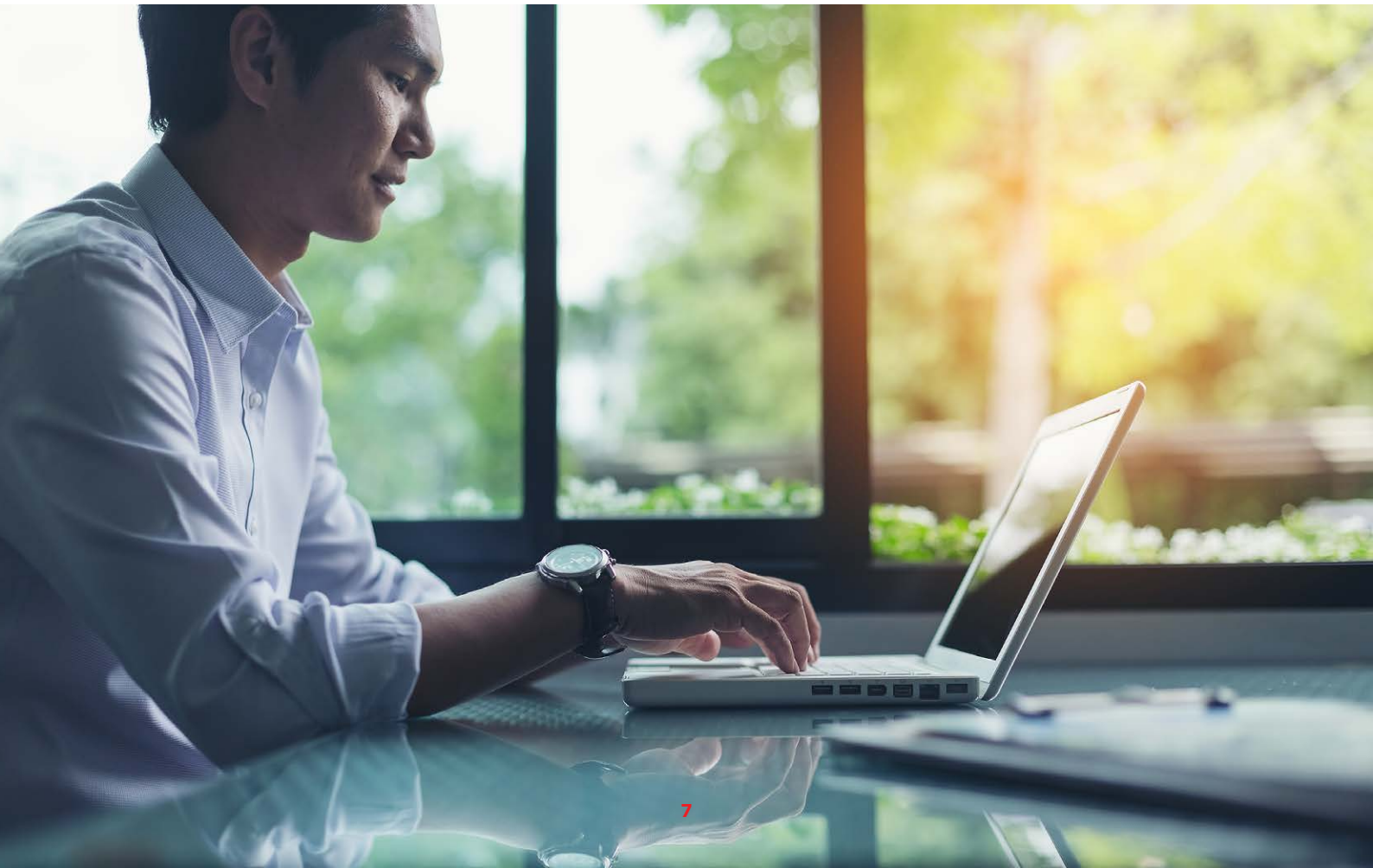
The skills mix required to address internal control is shifting and requires a broader range of expertise than may traditionally have been the case (as discussed in section 3.6) across all functions focused on internal controls (see section 1.3). Internal control can only be effective if those exercising it have the appropriate mix of skills, both at technical and interpersonal levels. The resourcing and make-up of both second- and third-line teams will be an issue as the scope of internal control expands. The purpose of internal control is discussed in section 1.2.

As the demands for the disclosure of information on aspects of the environmental, social and governance (ESG) and other agendas increase, so the level of assurance required on these disclosures likewise increases and they come into the scope of internal control (section 3.4). Nonetheless, at present, the data is less robust than for its financial counterpart: it derives from more varied sources and is often less structured. To address this concern, there is a need to invest in both the data and the skills, and hence, as across many aspects of internal control, there is a need to automate controls and reduce duplication; to encompass the elements of technology and to look forward.

Any part of this agenda requires the provision of guidance by relevant bodies, and an investment in continuing education initiatives by both entities and individuals.

Key observations

- The evolution of technology and control means that the gaps in the skill sets of those involved in internal control are significant issues, especially in relation to the breadth of skills across the lines.
- Technology will continue to advance and there is a risk that internal control becomes ineffective if it does not embrace the changes and automate where appropriate.
- If non-financial reporting is to be included within the scope of internal control, then there is a need to understand that the:
  - data is less robust and new methods of control need to be developed
  - sources of this data are more varied
  - embedding of controls is essential
  - levels of expertise need to be addressed.
- To embrace all these drivers, there needs to be an investment in the technology and data skills of those charged with internal control; there must be more relevant guidance that reflects current operating models as well as appropriate learning opportunities to support those working at all levels.

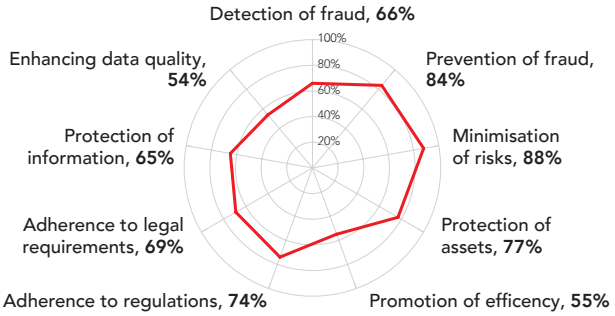


Internal control and the transformation of entities

This infographic provides a summary of the survey results from the joint internal control and transforming entities survey conducted in March 2022.

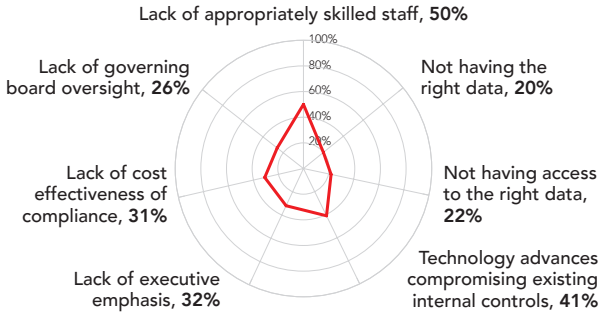
Purpose of internal control

What do we see as the purpose of internal control in an entity?



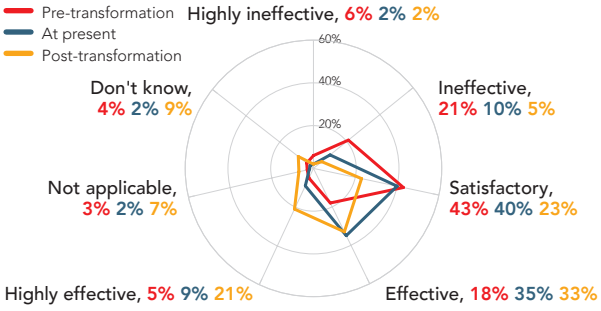
Challenges in internal control

What do we see as the challenges in internal control in our entities?



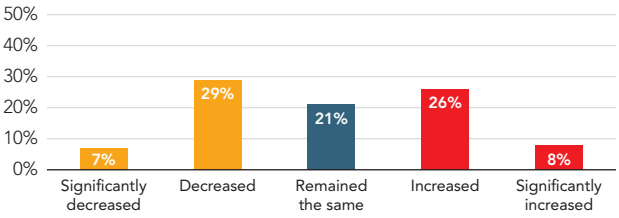
Impact of transformation on the effectiveness

What do we see as the impact of transformation on the effectiveness of internal control?



Impact of transformation on the risk

What do we see as the impact of transformation on the risks of internal control?



Internal control and ESG

Those who agree or strongly agree that they need to apply their internal control framework to non-financial and ESG reporting:

80%

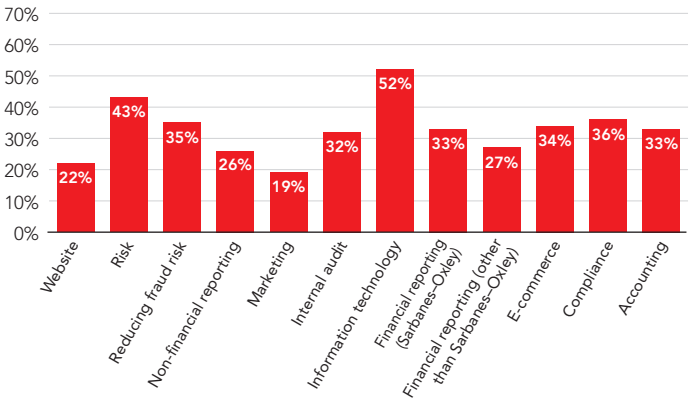
Key actions

Internal control in transforming entities gives rise to the following key actions:

1. Appreciate the forward movement of technology and data together with the impact on internal control.
2. Look to opportunities to embrace technology through automation and continuous monitoring.
3. Appreciate the need to include non-financial elements into internal control, accepting the need to develop new skills and the challenges of different data formats.
4. Develop the necessary skills, both technical and inter-personal, to be able to implement internal control in the transforming entity.
5. Implement skill development activities focused on control across the second and third lines.

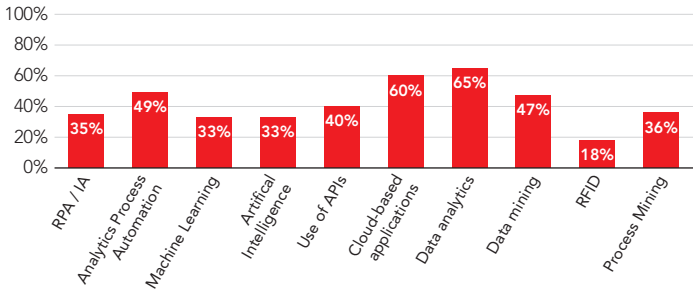
Significant effort required

What areas do we see as requiring significant effort post-transformation?



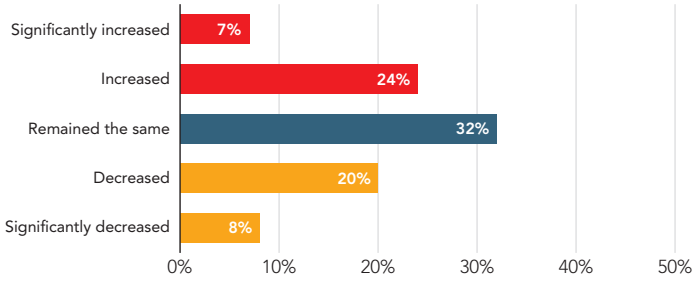
How technologies improve internal control

What is the extent to which the following technologies improve or significantly improve the internal controls?



Hybrid working

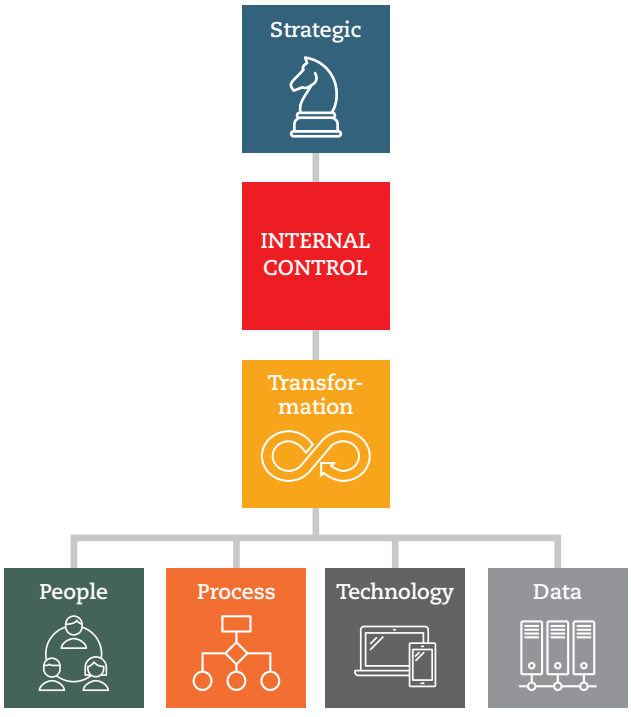
How did hybrid working impact the effectiveness of internal controls?



Key actions summary

This report makes several recommendations of actions to take to improve internal control. They are explained in the context of the detailed discussion in Chapter 3 and are collated in the table below, which also references them against the factors that are driving change in internal control for many entities (Figure ES1).

FIGURE ES1: Drivers for change for internal control



The key actions are as follows.

KEY ACTION	DRIVER(S)	SECTION
Consider the technology and data transitions which entities have integrated into the operating model and are reflecting these in the internal controls.		3.2
Ensure that you understand the technology and data drivers in the operating model of the entity. Ensure that you are familiar with the use of emerging technologies.		3.2
Map the use of emerging technologies to internal controls and identify opportunities to increase control effectiveness.		3.2
Appreciate that operating model developments are ever more likely to be conducted in an agile manner and ensure that those charged with internal control across all levels of the Three Lines Model are prepared to engage appropriately.		3.3
Reconfigure the risk model to reflect the changed technology practices that arise from the adoption of Cloud-based applications. Understand the different nature of the technology and of the vendor relationship.		3.3
Appreciate the internal control considerations arising from the changed risk profile in any Cloud-based scenario. Appreciate that the traditional information technology general controls (ITGCs) have changed.		3.3
Implement one GRC solution that addresses all elements of risk and internal control across the entity.		3.3
Embed automated and parameter-based internal controls into Cloud-based applications, especially at the point of initiation.		3.3
Work to identify the relevant data sources to enable the entity to meet the requirements of non-financial disclosures.		3.4
Develop a strategy to integrate the necessary non-financial data required into the internal control framework and be prepared to document as appropriate.		3.4
Liaise with those charged with data governance to ensure alignment across these data sets.		3.4
Re-evaluate the approach to automated controls within the entity.		3.5
Identify areas where manual controls are undertaken which may duplicate automated controls and eliminate as appropriate.		3.5

KEY ACTION	DRIVER(S)	SECTION
Understand the scope of end-user computing (including those outside the traditional definition) and ensure that all applications that are developed and that form part of the internal controls have the appropriate level of developmental and test controls applied to them.		3.5
Appreciate that agile transformation will increasingly require use of applications to develop enhancements to operating processes that are not subject to traditional application development life cycles and ensure that consequent risk is addressed.		3.5
Evaluate the IT general control environment in the context of the current operating model, identifying where controls are managed through Cloud-based rather than on-premises applications and the resulting changes in the risk profiles.		3.5
Appreciate the role that machine learning (ML) and artificial intelligence (AI) can play in the control environment.		3.5
Identify the skill sets and resources needed to sustain the effectiveness of internal control across the transformed entity, including skills needed to address non-financial objectives. Develop appropriate talent-management plans.		3.6
Consider your own level of technology and data-related skills in the context of internal control and identify relevant developmental opportunities.		3.6
Appreciate that skills need to be refreshed on a continuous basis, both in technology and in business acumen and interpersonal skills. Ensure that relevant initiatives are in place.		3.6
Develop and enact a strategy for continuous monitoring that is aligned to the expected data volume.		3.7
Ensure that there is an appropriate balance of manual and automated controls and seek to avoid redundancy and duplication in controls.		3.7
Ensure an alignment between the data governance and internal control objectives of the entity and strengthen procedures governing the completeness and accuracy of both financial and non-financial data.		3.8
Reinforce the importance of risk management and internal control on a continual basis across an entity.		3.9
Reinforce the need to be optimal in developing and implementing an internal control framework, especially as it is increasingly technology enabled.		3.9
Challenge the assumption that the 'computer is right' in all circumstances when considering internal controls.		3.9

TRANSFORMATION HAS FOUR ASPECTS: PEOPLE, PROCESS, TECHNOLOGY, AND DATA. THIS IS TRUE OF THE TRANSFORMATION OF INTERNAL CONTROL, AND IT IS IMPORTANT NOT TO LOSE SIGHT OF ALL THESE COMPONENTS IN THIS DISCUSSION.

1. Purpose of **internal control**

> **'KEEPING THE INTERNAL CONTROLS EFFECTIVE FROM A DESIGN AND OPERATIONAL PERSPECTIVE IN THIS FAST-CHANGING WORLD, WITH AGILE [APPROACHES] BEING CENTRAL TO THE TRANSFORMATION THAT ENTITIES MUST IMPLEMENT, PUTS A LOT OF CHALLENGE ON INTERNAL CONTROL ENVIRONMENTS TO BE RELEVANT AND TO BE MONITORING THE KEY RISKS IN A CONTINUOUS MANNER'.**
>
> ROUNDTABLE PARTICIPANT FROM TÜRKIYE

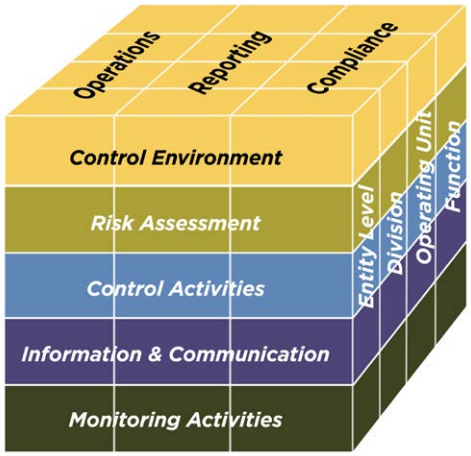
1.1 Origins of internal control

The term 'internal control' was first defined by the American Institute of Accountants (now the American Institute of Certified Public Accountants) in 1949. The Institute further refined this definition in 1958 and 1972 (Lauren 2017). The definition offered was:

'Internal control comprises the plan of organization and all of the co-ordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies' (cited in Heier et al. 2005).

A series of corporate challenges in the 1970s led the US Securities and Exchange Commission (SEC) and the US Congress to enact the Foreign Corrupt Practices Act in 1977. As a response to this, several entities in the US, including The IIA and IMA, worked together under the chair of James C. Treadway, Jr., then executive vice president and general counsel at Paine Webber and former commissioner of the US SEC, to develop a framework for internal control. The Committee of Sponsoring Organizations of the Treadway Commission (commonly known as COSO) developed its framework, which was updated in 2013. A summary of the COSO framework is shown in the model below (Figure 1.1).

FIGURE 1.1: COSO Framework



Source: COSO (2013)

The 2013 revision to the framework provides the following updated definition.

Internal control is 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.

This definition reflects certain fundamental concepts. Internal control is:

- *Geared to the achievement of objectives* in one or more categories – operations, reporting and compliance
- *A process* consisting of ongoing tasks and activities – a means to an end not an end in itself
- *Effected by people* – not merely about policy and procedure manuals, systems and forms, but about people and the actions that they take at every level of an organization to effect internal control
- *Able to provide reasonable assurance* – but not absolute assurance, to an entity's senior management and board of directors
- *Adaptable to the entity structure* – flexible in application for the entire entity or a particular subsidiary, division, operating unit or business process.

Source: COSO (2013)

As noted, the 2013 COSO Internal Control Integrated Framework has five components (Control Environment; Risk Assessment; Control Activities; Information and Communication; and Monitoring), with the last component being particularly important to support agility, timeliness and automation in a rapidly changing and disruptive business environment.

The COSO framework also has 17 principles (Figure 1.2). Generally, for internal controls to be effective, these principles must be present, functioning and integrated.

In updating the 1992 landmark internal control framework, the COSO 2013 framework was enhanced by expanding the financial reporting category of objectives to include other important forms of reporting, such as non-financial and internal reporting (for example, sustainability reporting and analysis).

Other jurisdictions have developed similar definitions of the concept. As an example, in the UK, the *Internal Control: Guidance for Directors on the Combined Code* (known as the Turnbull Report, FRC 2005), first published in 1999, defined internal control and its scope as follows:

'The policies, processes, tasks, behaviours and other aspects of an organisation that taken together:

- 'Facilitate effective operation by enabling it to respond in an appropriate manner to significant business, operational, financial, compliance and other risks to achieve its objectives. This includes safeguarding of assets and ensuring that liabilities are identified and managed.
- 'Ensure the quality of internal and external reporting, which in turn requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from both internal and external sources.
- 'Ensure compliance with applicable laws and regulations and also with internal policies' (ICAEW 1999).

It is within this context that this report looks at internal control and how it is affected by several changes that entities face. The intent of these frameworks and guidance remains valid, but the next and more challenging step is in the practical implementation. The report does not seek to comment on any one model against another, rather it is agnostic of the models themselves and focuses on the implementation experiences of the practitioners surveyed and interviewed.

FIGURE 1.2: The COSO Internal Control – Integrated Framework Principles

CONTROL ENVIRONMENT	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
RISK ASSESSMENT	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
CONTROL ACTIVITIES	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
INFORMATION & COMMUNICATION	13. Uses relevant information 14. Communicates internally 15. Communicates externally
MONITORING ACTIVITIES	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Source: COSO (2013)

1.2 Perceptions of its purpose

The research started by considering what the survey respondents perceived as the purpose of internal control in their entities (Figure 1.3).

The survey respondents saw prevention of fraud (84%) and the minimisation of risk (88%) as the main factors that described the purpose of internal control. Data quality was the lowest-ranked factor among those from which the respondents could select (54%), although the connection between internal control and data governance was an issue frequently raised in the roundtable discussions and is a theme that will be returned to later in this report (see section 3.8). A regional analysis of the survey results confirmed a similar pattern.[2]

An Australia roundtable participant described internal control as follows. 'It's really covering three things as far as I am concerned. It is about making sure that, firstly, information is reliable and accurate. We need to ensure that we are complying with accounting standards, regulations, policies, etc. The third thing is its reliability around financial reporting. Extending from those three attributes is data and technology, which are driving regulatory changes'.

The survey respondents were asked to consider the challenges their entity's face with internal control[3] (Figure 1.4). At a global level, the lack of appropriately skilled staff was ranked as the most significant challenge, with 50% of respondents selecting this (the skill sets are further discussed in section 3.6). There were contrasts in the responses by region, with 42% of respondents in Western Europe selecting this factor in contrast to 56% in North America and 58% in Asia–Pacific, 50% in Africa and 54% in the Caribbean. Skill sets, especially in the context of technology and the environmental, social and governance (ESG) agenda, were also raised by several roundtable participants.

FIGURE 1.3: In your opinion, which of these factors describes the purpose of internal control? Select all that apply (n = 1,956)[1]

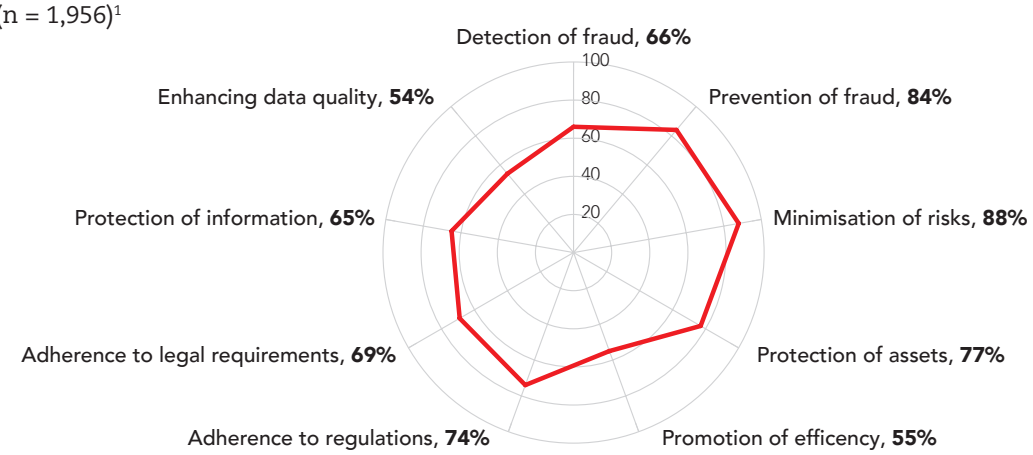
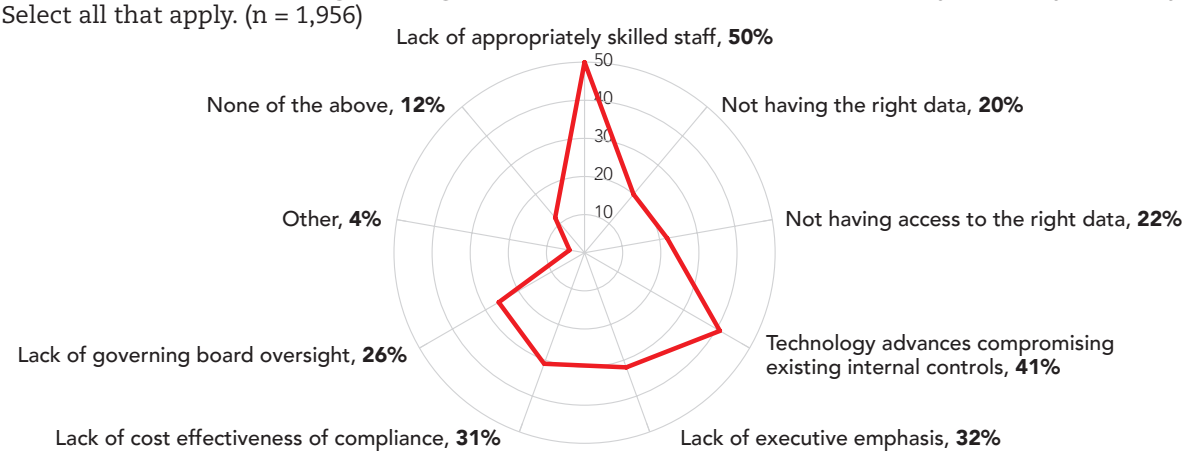


FIGURE 1.4: Which of the following challenges in an internal control framework does your entity currently face? Select all that apply. (n = 1,956)



1 All statistics used in this report come from the ACCA / IIA / IMA Transformation of Internal Control survey, March 2022, unless otherwise stated.
2 Several analyses of selected survey results by location or sector accompany this report in a series of infographics.
3 Definitions of key terms used in this report are given in the Glossary.

Among our respondents, 41% considered that advances in technology compromise internal controls. This was broadly similar across all the regions. Considering the impact of technology and data across entities this level was not surprising, although only a small proportion (20%) claimed that they did not have the right data and only 22% considered that they did not have access to this data.

Reports of a lack of governing board oversight, cited by 26% overall, showed some variation when considered at the regional level. In Western Europe (20%) and North America (17%) there was a stronger sense of the lack of oversight than in the Middle East (which recorded 37%), South Asia (30%) and Asia–Pacific (33%). The variation may, in part, be due to variations in the culture of internal control and risk management between locations (the importance of culture and its relationship to internal control is, again, considered later in this report, in section 3.9).

Commenting on the lack of appropriately skilled staff, a chief audit executive based in Europe explained that 'the biggest challenge that we are currently facing is that there are not [enough] sufficiently skilled people to keep up with the changes in technology'.

An Australian roundtable participant explained their perception of the challenges as, 'what a lot of companies are facing now is an audit challenge in that we run the risk of automating inefficient processes, because that is the way we have always done it. We are not keeping pace [with] change'. One potential weakness with transformations is simply to automate an existing process without optimising the process first. The application of technology alone can never, of itself, improve a process. A similar inference can be made with respect to the automation of controls.

1.3 The Three Lines Model

In 2008 – 2010 the Federation of the European Risk Management Associations and the European Confederation of Institutes of Internal Accounting published a three lines of defence position paper to enhance the understanding of governance, risk management and control by clarifying roles and duties. This was developed as guidance for the 8th EU Directive Art. 41 2b[4]. In 2020 IIA refined 'The Three Lines', which can be briefly described as follows.

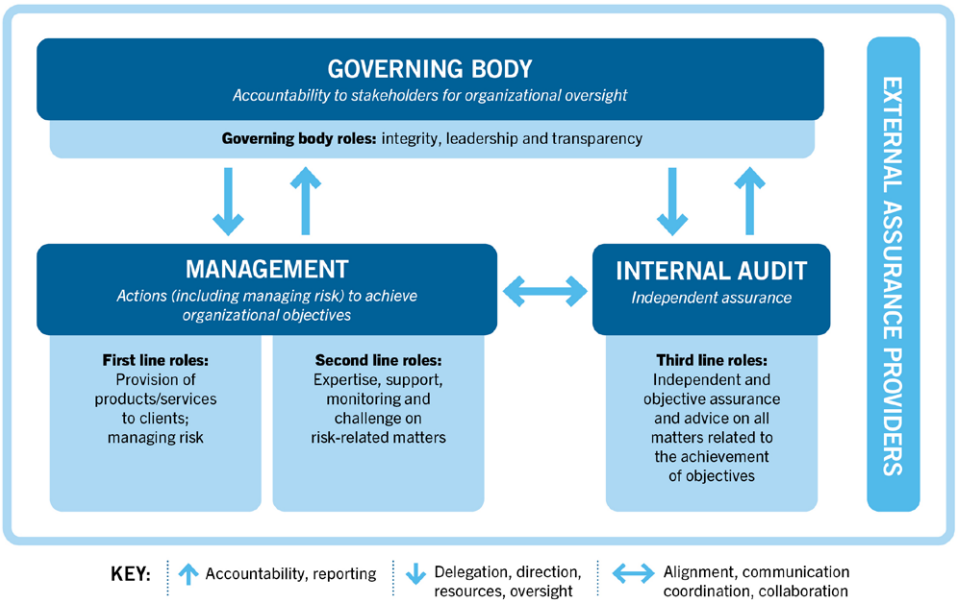
The Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. The model applies to all organizations and is optimized by:

- Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of "defense" and protecting value.
- Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- Implementing measures to ensure activities and objectives are aligned with the prioritized interests of stakeholders.

Source: IIA (2020)

The Three Lines are represented in the following figure (Figure 1.5).

FIGURE 1.5: The IIA's Three Lines Model



Source: IIA 2020

4 The evolution the Three Lines Model is considered in Sheen (2020). A commentary was provided by ACCA in Ashby et al (2019).

Survey respondents were asked to rank the effectiveness of each of the key players with respect to their roles (Figure 1.6). The results show a broadly consistent pattern, with strong support for each of the elements of the model. At a regional level, there was a broad consistency with the global results.

The Three Lines Model does not suggest giving one business function priority over another but, to give a better sense of the areas on which survey respondents commonly placed the most emphasis, they were also asked to rank the business functions in order of importance to their entity on a scale of 1 to 5, where 1 represented the most important, and 5 the least (Table 1.1).

The results show that compliance with laws and statutory regulations is a requirement, however, there is additional focus on increasing financial integrity. Monitoring procedures scored the lowest but was still seen as relevant.

For many roundtable participants and interviewees, the cost effectiveness of internal control was a major consideration. That internal control is perceived by their leadership as a cost rather than a benefit, especially in more lightly regulated environments, created many challenges. One chief financial officer (CFO) based in the US commented that educating people about the purpose and benefits was essential, adding that 'this needs to happen right from the third line of defence? Or from the second line. You know the first line in the business, and you need to let them know the importance of doing this and how.'

A lead auditor in the financial services industry commented: 'Control tends to be the boring part because it is time consuming, it is onerous and [people] want to do other things that are less invasive so that can be effective in their day. Technology is a way to enable them to overcome that'.

FIGURE 1.6: Considering The Institute of Internal Auditor's Three Lines Model (2020), please rank the respective effectiveness of each line with respect to their role (n = 1,956)

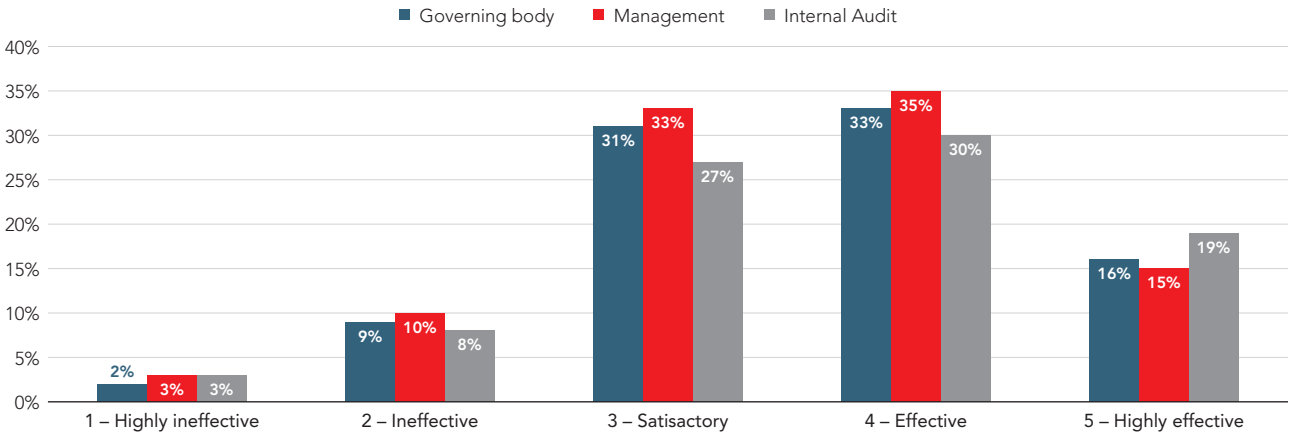
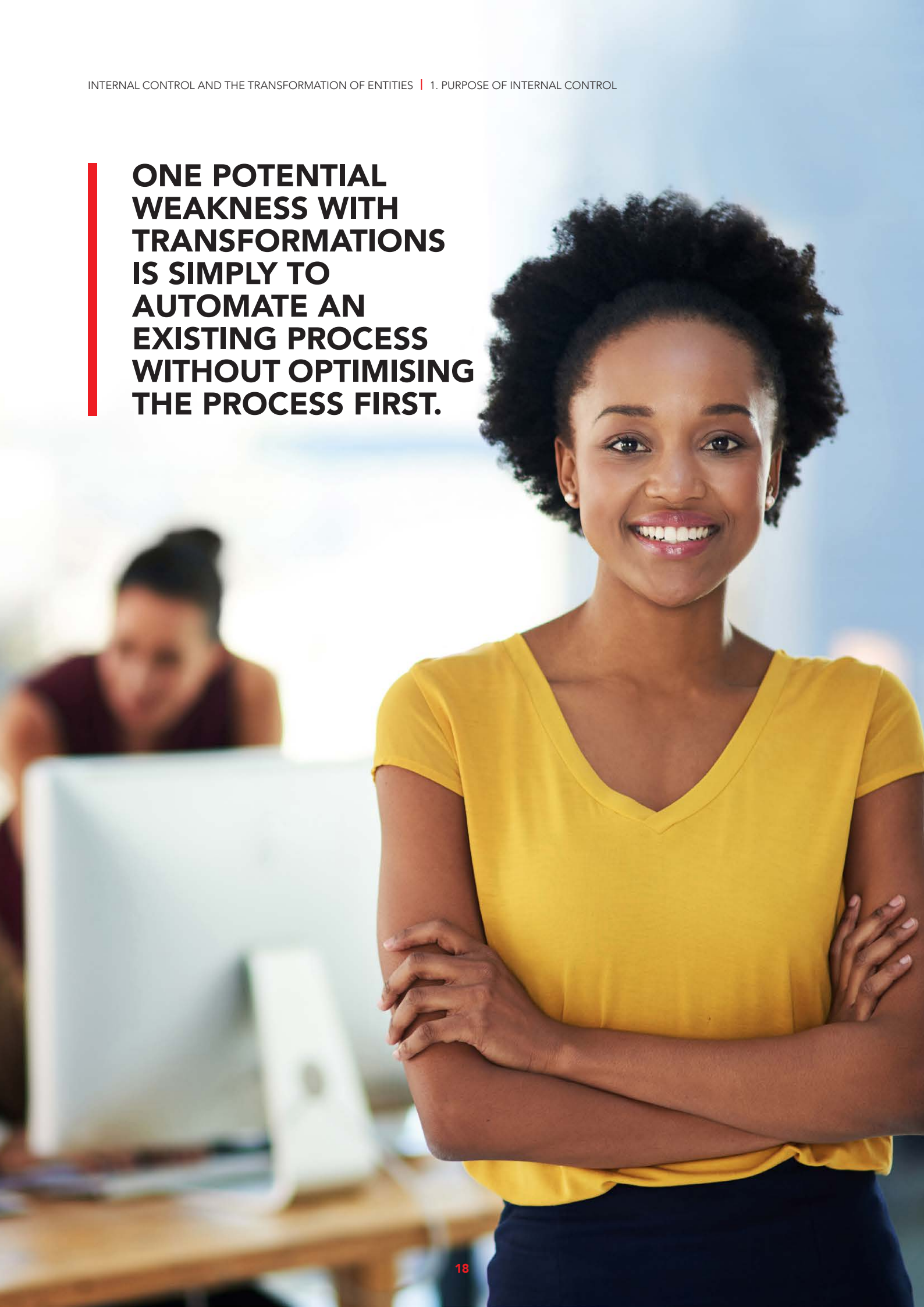


TABLE 1.1: Please rank the following elements of the Three Lines in order of most to least important for your entity, where 1= the most important; 5 = least important (n = 1,956)

	AVERAGE RESPONSE SCORE
Establishing monitoring procedures	3.43
Ensuring compliance with laws and statutory regulations	2.49
Increasing financial reliability and integrity	2.85
Helping protect assets and reduce the possibility of fraud	3.06
Improving efficiency in operations	3.11

ONE POTENTIAL WEAKNESS WITH TRANSFORMATIONS IS SIMPLY TO AUTOMATE AN EXISTING PROCESS WITHOUT OPTIMISING THE PROCESS FIRST.



2. Current **challenges** and **opportunities**

'WE MUST BE ABLE TO UNDERSTAND HOW PERVASIVE OUR CONTROLS NEED TO BE. WE MUST BUILD IN CONTINUOUS MONITORING AND ANALYTICS. WE MUST AUTOMATE AS MUCH AS POSSIBLE'.

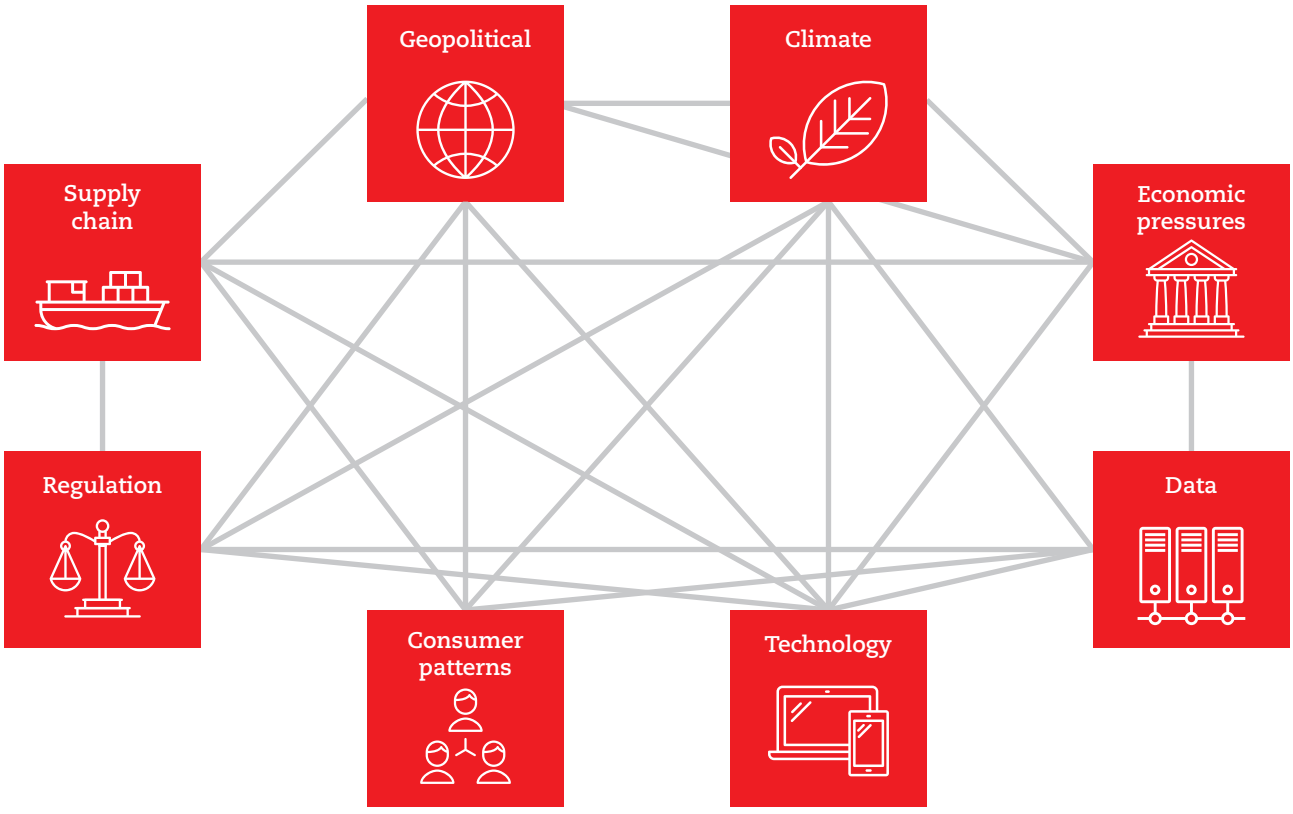
CHIEF AUDIT EXECUTIVE PARTICIPATING IN THE CARIBBEAN ROUNDTABLE

2.1 Impact of transformation

Entities have experienced a significant amount of disruption in the past two years. The pandemic has created many challenges and, in many cases, forced necessary changes to business models. There are many ways of viewing transformation in entities and ACCA (ACCA / CA ANZ / Generation CFO 2021), IIA (IAF / Auditboard 2020) and IMA (Jiles 2021) have explored this topic in their research papers. These reports stress the continuous nature of transformation for entities and the need to ensure that they can benefit from agile approaches to rapidly address current challenges. The continuous cycle of transformation embraces the application of technology and data-driven approaches, accepting that neither can be the primary driver for transformation itself.

Internal control, like the entities themselves and their transformational objectives, is subject to complex network of drivers of change (Figure 2.1). While each of these may have a substantive impact, in combination they represent a period of turbulence for most entities. This is a time when risks are high and the need for controls to be effective is paramount.

FIGURE 2.1: Drivers of change potentially disrupting internal control



This report is concerned with the impact of these transformation activities on the internal controls of entities. As a benchmark, it was important to understand the breadth of transformational activities across the respondents' entities (Figure 2.2).

In most cases, the respondents either had some form of transformational activity under way or planned. For nearly a quarter of respondents, their transformational journey for accounting had started four or more years previously, while only 16% had either no activity planned or were not aware of any. These results underline the shift that entities are undertaking to remain relevant.

Any transformation is made up of several elements: people, process, data and technology. The definitions of internal control reflect a similar breadth and hence it is inevitable that the internal control environment of an entity will itself be changed by these transformational activities.

The survey respondents were asked how they considered that the internal control risk may have changed because of these transformation activities (Figure 2.3).

The results show that 36% globally claimed that transformation had either decreased or significantly decreased the internal control risk in their entities, although 34% claimed that it had either increased or significantly increased the risk. This balance may in part be due to other factors, such as a level of understanding of the technologies implemented and the impact of the changes on ways of working and the effectiveness of the change management activities. Transformations are challenging. Having a clear alignment to the strategic goals of the entity and communicating the change effectively are both essential for any such activity to be successful. Allowing for the impact of these activities on the control environment can be challenging.

FIGURE 2.2: Please indicate whether transformation activity has occurred, or is planned in the following areas of your entity (n = 1,956)

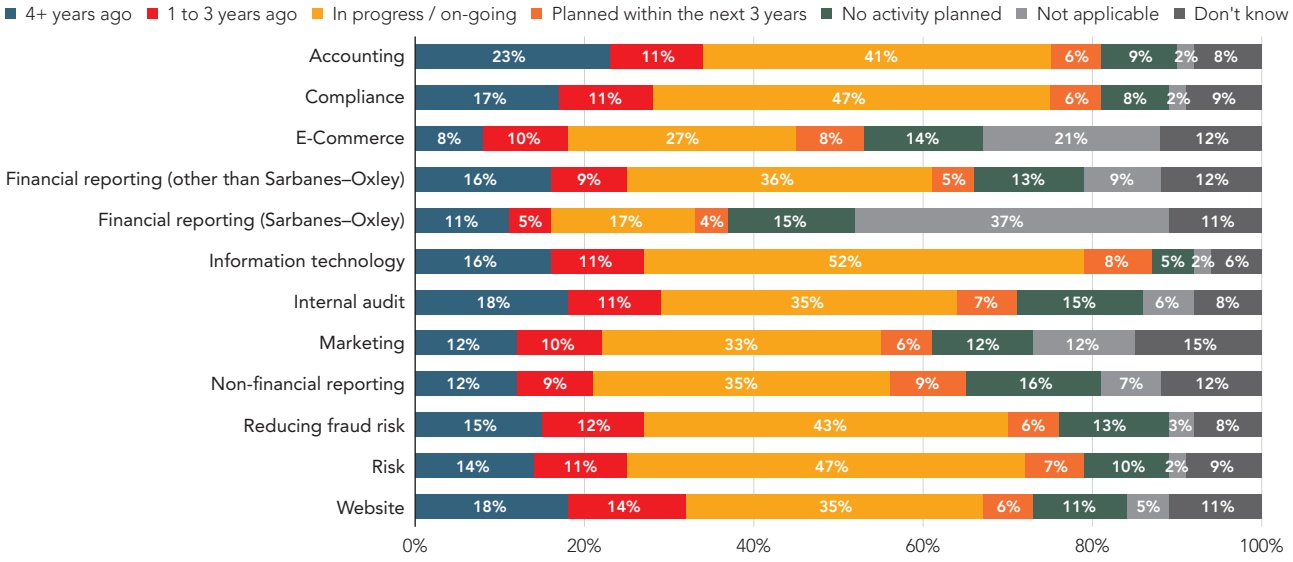
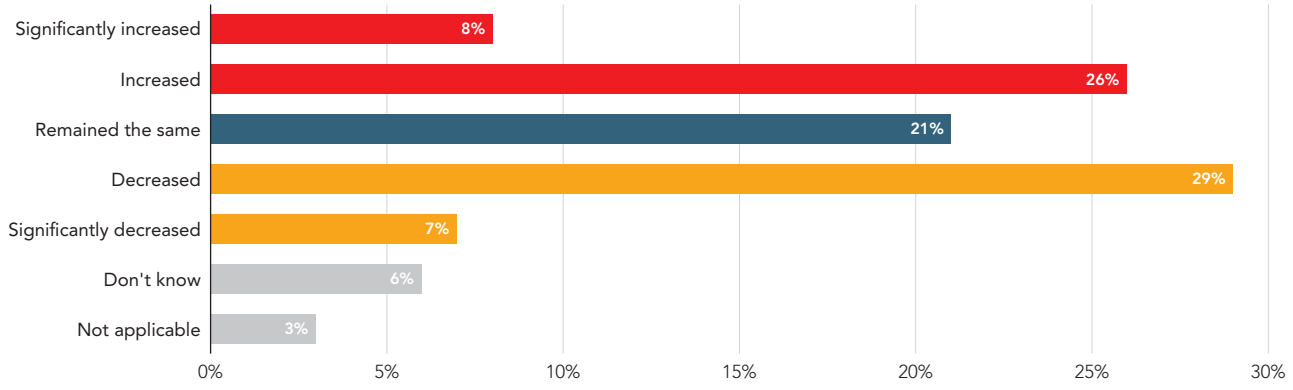


FIGURE 2.3: In general, did internal control risk ultimately increase, decrease, or stay about the same because of transformation activities? (n = 1,833)



An analysis of the differences between the ultimate impact on internal control risk of transformation in different regions shows some variations (Figure 2.4).

The nature of the variations may, in part, be due to the differing cultural attitudes to internal control as to whether it is seen as principally a compliance driven activity or an effectiveness led activity. The nature of the transformations themselves, and the diverse nature of the business environments will also be contributing factors.

The survey respondents were asked to consider the overall effectiveness of internal control during a transformation process (Figure 2.5). From the results, it can be seen that the respondents reported that there had been a shift in the overall perceived effectiveness of internal control because of the transformational activities that their entities had undertaken. Whilst this may well be anticipated, and indeed a result which indicated the reverse would be a remarkable outcome, the roundtable participants and interviewees reflected upon several challenges as outlined in section 3.5.

FIGURE 2.4: In general, did internal control risk ultimately increase, decrease, or stay about the same because of transformation activities? Analysis by region (n = 1,833)

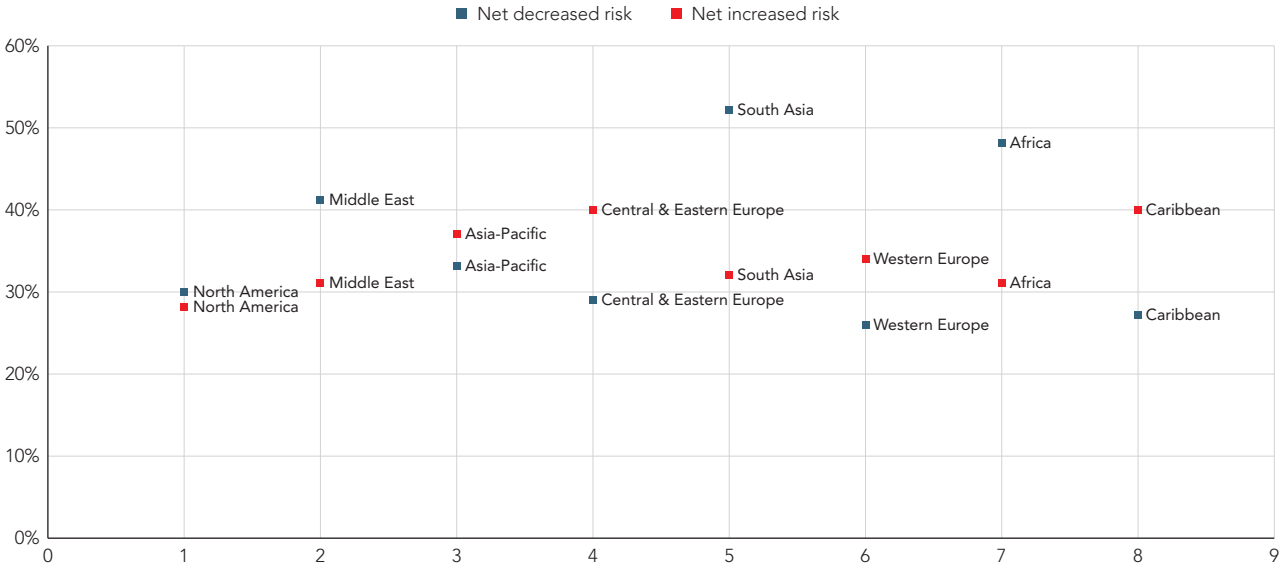
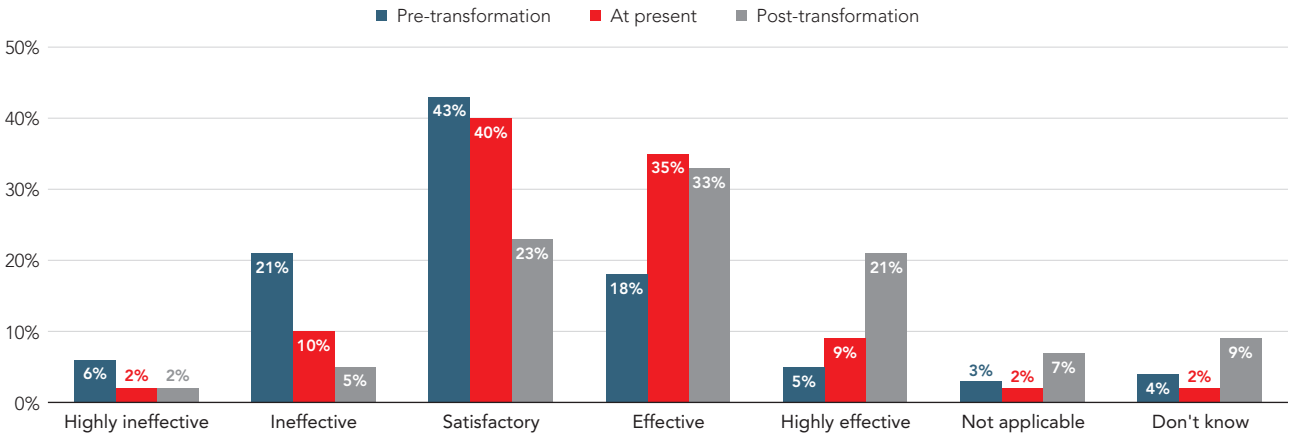


FIGURE 2.5: How would you rate the overall effectiveness of the internal control framework in your entity throughout the transformation process? (n = 1,833)



A further analysis of the results focuses upon the change in those who gave one response in a pre-transformation scenario to that which they gave in a post-transformation one (Table 2.1).

The survey results would suggest that the overall perception is that transformational activities have a positive benefit on the internal control environment as the number of those who assess it as highly ineffective decreases because of the activity; while the number who see it as effective, increases.

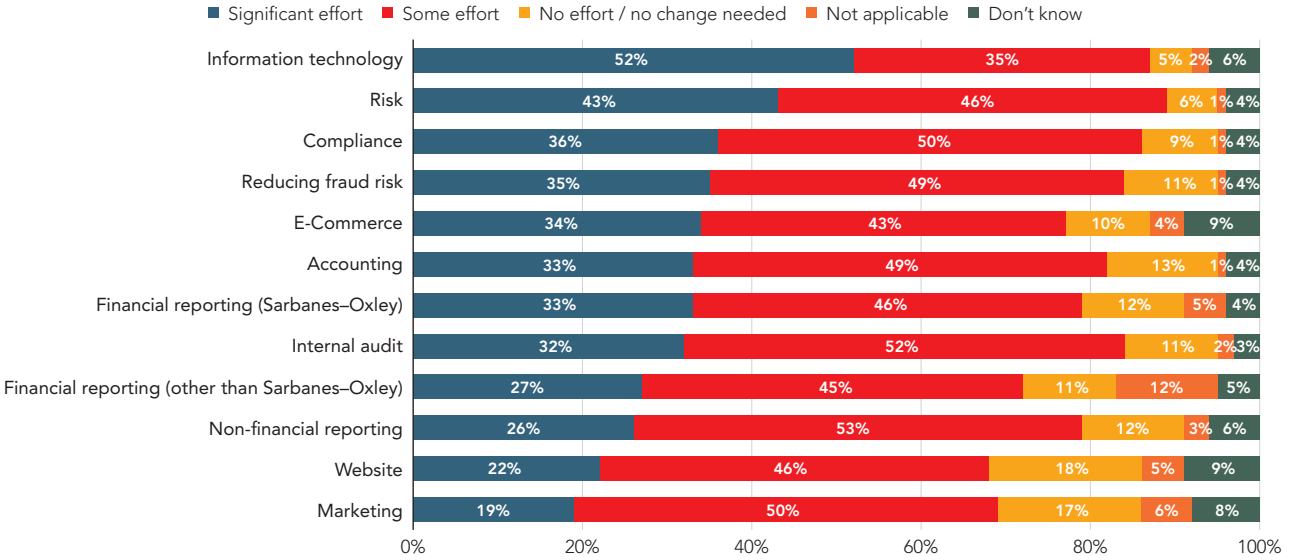
A further question (Figure 2.6) asked respondents to consider the extent of the effort required to improve the internal controls because of transformation activities. As can be seen from the figure, in all areas a degree of effort was required. For example, for accounting, 33% of the respondents reported that a significant effort was required and a further 49% considered that some effort was needed. Marketing (19%) was the area evaluated as requiring the least significant effort.

TABLE 2.1: Comparison of pre- and post-transformation effectiveness assessments

(To interpret this table, as an example, 7% of those who rated their internal control framework highly effective pre-transformation do not know their evaluation post-transformation; while 68 % of those who rated the pre-transformation control framework 'highly effective' gave it the same rating post-transformation).

POST-TRANSFORMATION	PRE-TRANSFORMATION REALLOCATED TO RATING POST-TRANSFORMATION				
	Highly ineffective	Ineffective	Satisfactory	Effective	Highly Effective
Highly ineffective	20%	2%	1%	1%	0%
Ineffective	15%	14%	1%	1%	2%
Satisfactory	24%	26%	32%	10%	8%
Effective	21%	36%	32%	51%	13%
Highly effective	8%	10%	23%	29%	68%
Not applicable	7%	9%	4%	2%	2%
Don't know	5%	3%	7%	6%	7%

FIGURE 2.6: How much effort (time and complexity) was needed to update internal controls in response to transformation activities in each of the following areas?



The responses for each of the sub-questions was as follows (n=)

Accounting	Compliance	E-commerce	Financial reporting (Sarbanes–Oxley)	Financial reporting (other than Sarbanes–Oxley)	Non-financial reporting	Reducing fraud risk	Information technology	Internal audit	Marketing	Risk	Website
1,469	1,469	874	638	1,206	1,089	1,352	1,551	1,237	1,071	1,410	1,310

The respondents were also asked what the extent of the challenges were in updating their internal controls (Figure 2.7). The respondents reported that each of the areas suggested was a challenge. Lack of technical knowledge was reported as either challenging or extremely challenging by 45% of respondents while 41% considered that a lack of focus on internal control was also an issue. In South Asia 57% of the respondents, and 54% in the Middle East, considered that lack of technical knowledge was a challenge, in comparison with 35% in the Caribbean, 38% in Western Europe and 40% in North America.

A US-based internal audit lead commented, 'we really need to move the [conversation about] control to the beginning: [to] think about that and make sure it gets implemented every time there is a new process or service.'

A chief audit executive from South Africa commented: 'we tend to see business process investments and internal control investments as two separate things from a technology point of view. I don't see it as separate as perhaps we used to traditionally see it. It is more [a question of] how are you in improving your business process environment with technology and how it works? Are we thinking enough about improving in internal controls every time we make a technology investment?'

An Australian roundtable participant commented: 'As internal auditors we need to always be conscious as the [technologists] usually do not think from a controls point of view'.

Operating in a constantly changing world has other impacts that may well affect the internal control environment. The traditional model of planning and forecasting has been challenged in many entities. The ability to model various scenarios by using data from many sources has served those involved well during the pandemic.[5]

Classically, monthly reporting cycles have been an area with very focused internal controls. While there has been discussion on streamlining some of these processes (see Krumwiede 2016) many of the traditional activities remain, albeit on a shorter timescale. The survey respondents (Figure 2.8) indicated that, because of the pandemic, monthly reporting cycles have indeed continued to become more relevant.

FIGURE 2.7: To what extent did each of the following cause challenges when updating your internal controls as a result of transformation? (n = 1,836)

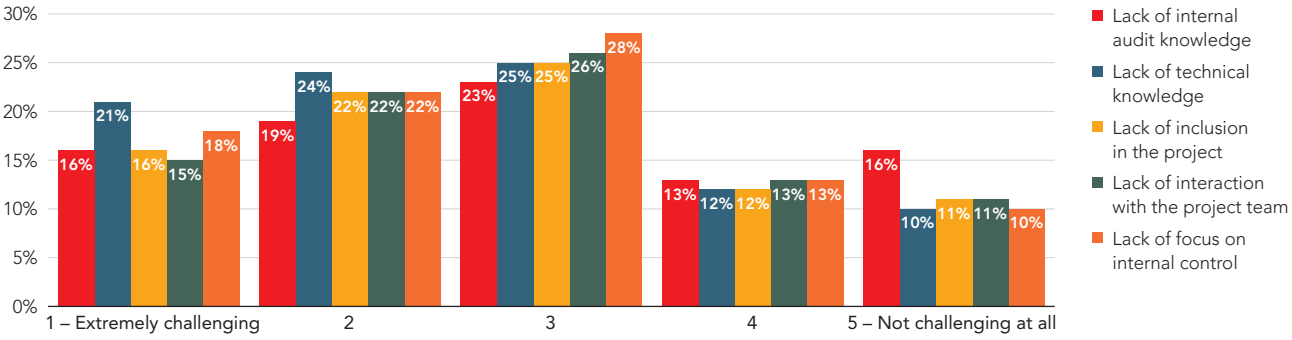
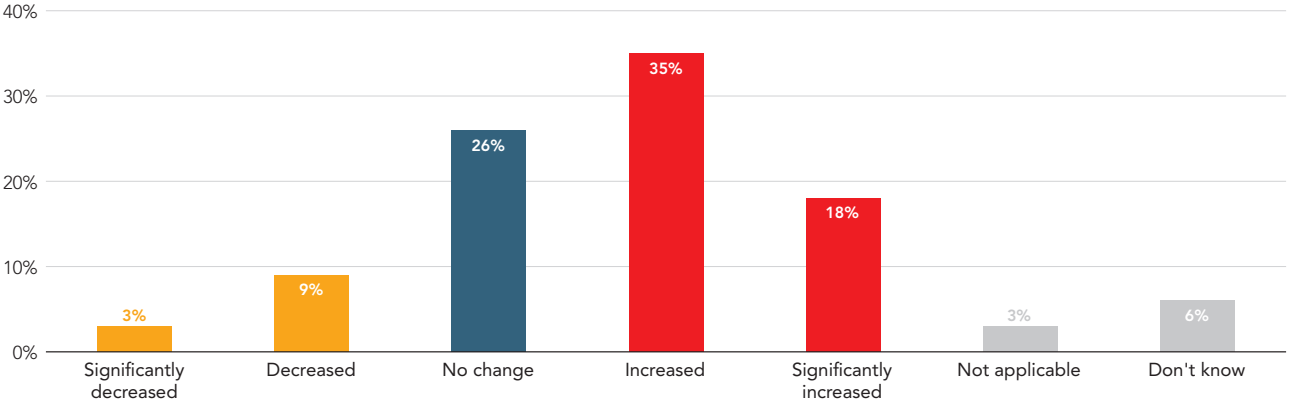


FIGURE 2.8: As many entities look towards more real-time decision making, how would you consider the relevance of monthly reporting cycles in comparison to 2019? (n = 1,956)



5 A consideration of the impact of the pandemic on planning and forecasting is contained in ACCA / PwC (2021).

A regional analysis of the responses to this question shows variation when comparing net increased and net decreased relevance (Figure 2.9).

2.2 Technology adoption

An entity's transformation activities have an impact on finance in many ways. The reality of transformation is that it is not a department-level activity, it is an entity-wide one which has varying impacts in different areas. The post-pandemic challenges for entities in certain economies can be reflected as a shortage of talent, as individuals seek to reappraise their expectations from life. With inflationary pressures also growing, the drivers for automation increase and the ability of transformation initiatives to enable this is becoming increasingly important.

It is against this background that the survey respondents were asked to evaluate the impact of a range of technologies[6] on the internal controls of their entities (Figure 2.10).

FIGURE 2.9: As many entities look towards more real-time decision making, how would you consider the relevance of monthly reporting cycles in comparison to 2019? Analysis by region (n=1,956)

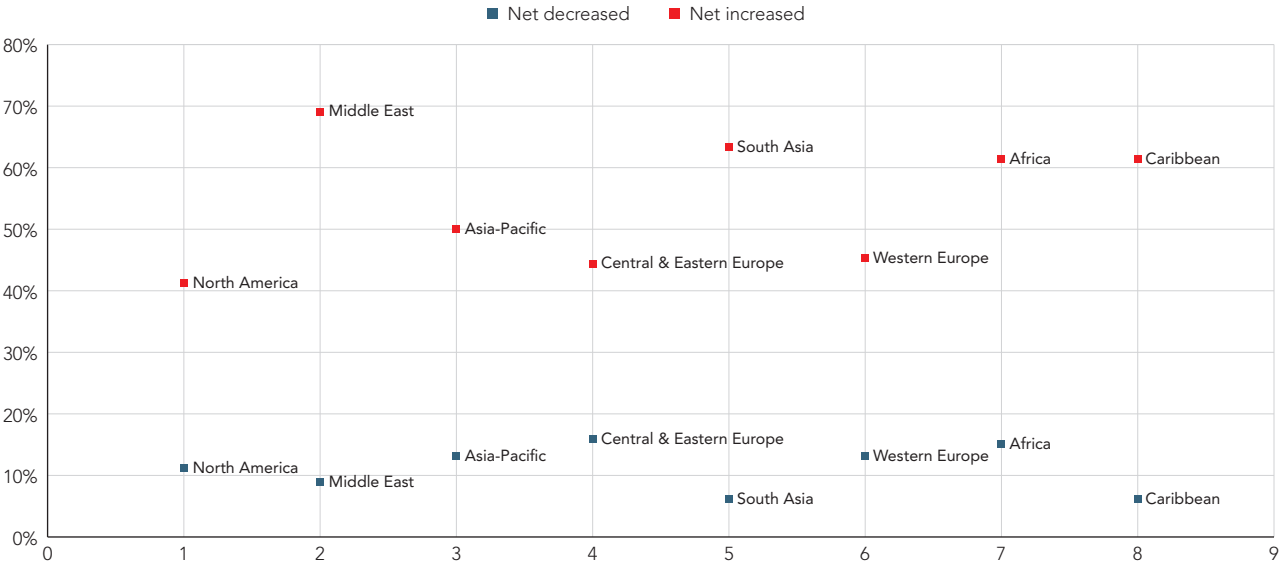
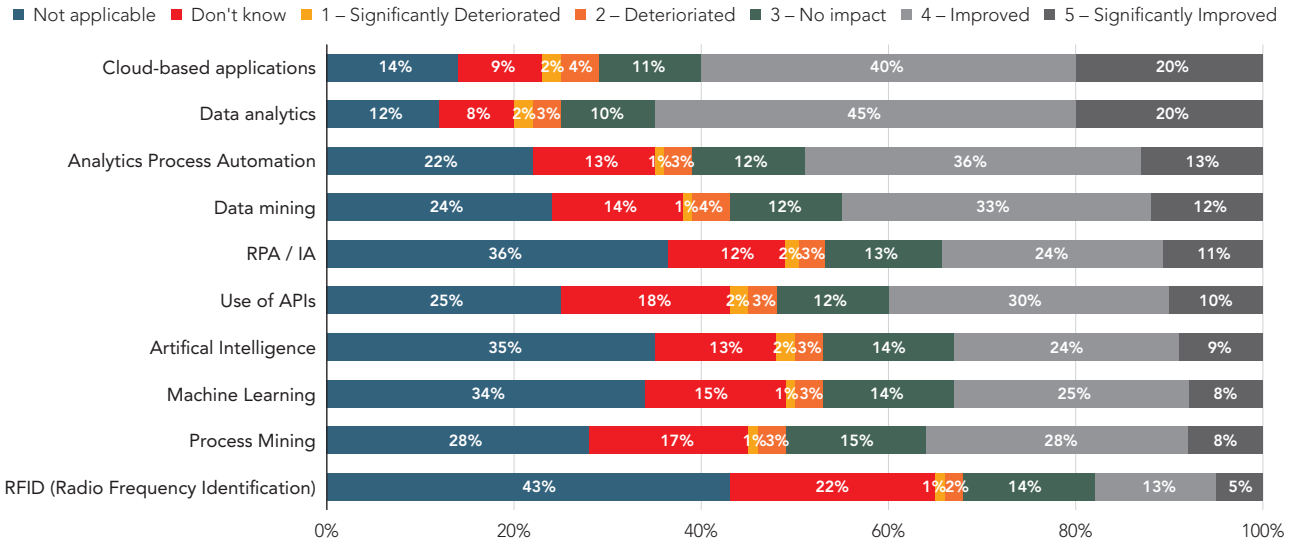


FIGURE 2.10: How would you evaluate the impact of the following technologies on the internal controls of your entity? (n = 1,956)



6 Explanations of a number of these terms, together with other key terms used in this report are given in the Glossary.

The results are variable. In certain cases, tools such as robotic process automation and intelligent automation (RPA / IA) are either not applicable or their impact unknown to 48% of the respondents, while 34% of the respondents considered that the same technologies had improved their internal controls. A similar pattern appears for many of the technologies referenced in this question. Only data analytics and Cloud-based applications score significantly higher, with 65% recording either an improvement or significant improvement because of data analytics and 60% for Cloud-based applications. The great divides in responses for specific technologies reveal the varied stages of exposure to, and implementation of, each of these in digital transformation initiatives. Taken together with the commentary provided by the roundtable participants, the survey results imply that, for accountancy, finance and internal audit professionals, there remains a journey to understand and apply technology to our entities.[7] The implications of this are considered further in Chapter 3.

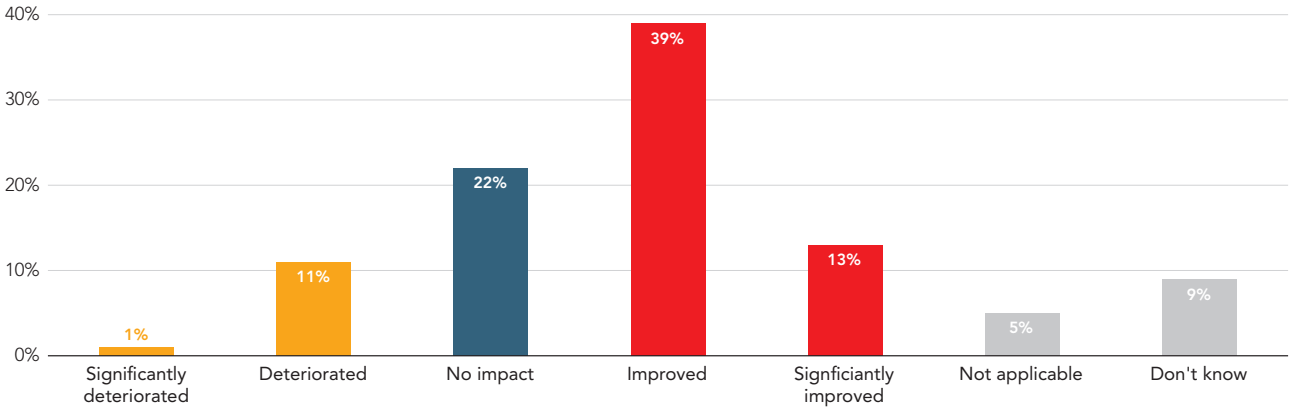
2.3 Data flows, big data and continuous monitoring

According to a Statista forecast in 2021, the world will create 97 zettabytes[8] of data in 2022 and this will rise to 181 zettabytes in 2025 (Statista 2021). This explosion of data is one aspect of the transformation journey for many entities as they seek to use data in ways that enable them to understand their customers better, among other activities, and streamline their processes. This increase in data is driven by the so-called 'fourth industrial revolution'[9] and the connected world. Each of these activities can, in part, be supported by the technologies cited in Figure 2.10.

The survey respondents were asked to consider whether this massive increase in available data had changed the effectiveness of their entity's internal controls (Figure 2.11).

Among our respondents, 52% reported that the increased availability of data had helped by improving the effectiveness of internal control. This level of improvement was greatest in Asia–Pacific (57%), South Asia (60%) and the Middle East (63%), whereas the figures were lower in Western Europe (44%) and North America (37%).

FIGURE 2.11: Many entities capture more data in comparison to five years ago. Much of this data is relevant to both financial and non-financial reporting. Has this increase in the volume of data impacted the effectiveness of the internal controls? (n = 1,956)



AMONG OUR RESPONDENTS, 52% REPORTED THAT THE INCREASED AVAILABILITY OF DATA HAD HELPED BY IMPROVING THE EFFECTIVENESS OF INTERNAL CONTROL.

7 The implications of technology for the skill sets of accountancy and finance professionals are discussed in ACCA (2020).

8 A zettabyte is a multiple of the unit byte that measures digital storage, and it is equivalent to 1,000,000,000,000,000,000,000 [10^{21}] bytes.

9 The term 'fourth industrial revolution' was first introduced to a wide audience by Klaus Schwab in an article in *Foreign Affairs* in 2015 (Schwab 2015).

One of the challenges with such volumes of data is that traditional sampling techniques become challenged in ensuring that appropriate conclusions are drawn from testing – several roundtable participants referred to this. The opportunity to use computing power to constantly review the totality of a population, so called 'continuous monitoring', may offer advantages in internal control monitoring. Of the survey respondents 28% were already using this technique and a further 36% were considering it (Figure 2.12). The implications of continuous monitoring are considered in Chapter 3.

2.4 Evolving ways of working

Transformational changes are not related only to technology and data. Rather, they are often fundamental shifts in the ways of working. One lesson from the pandemic is that those entities that have managed the challenges more effectively are those that have adopted collaborative and innovative cultures.

Another aspect has been the shift to hybrid working that has been seen in many entities, especially for more office-based staff members. At the start of the pandemic, questions were raised about the impact of home or hybrid working on the internal control environment. Would it be robust? While there have been challenges (and some of these and their control implications will be explored in Chapter 3), the survey respondents considered that overall the effectiveness of the controls had either increased or remained the same with only 31% reporting that it had either decreased or significantly decreased (Figure 2.13). Nonetheless, while in Asia–Pacific (30%), South Asia (33%) and Western Europe (25%) there was an impression that controls had been improved, only 15% of the respondents in North America considered this to be the case.

A roundtable participant from Türkiye commented: 'working from home as opposed to the office would not make really big change from [a] control perspective. I guess the assessment might be different because it all depends on how well the control environment is structured. If you have automated controls in place much more than your manual controls and your systems are integrated, then working from anywhere has nothing to do with the control environment'.

FIGURE 2.12: With the increasing availability of Big Data, is your entity considering the use of, or using, continuous auditing and / or continuous monitoring techniques as part of their internal controls? (n = 1,956)

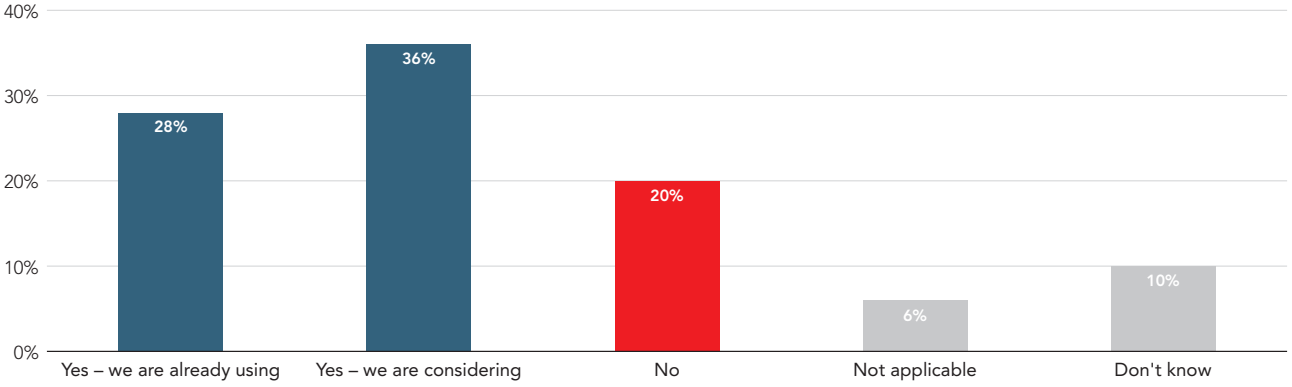
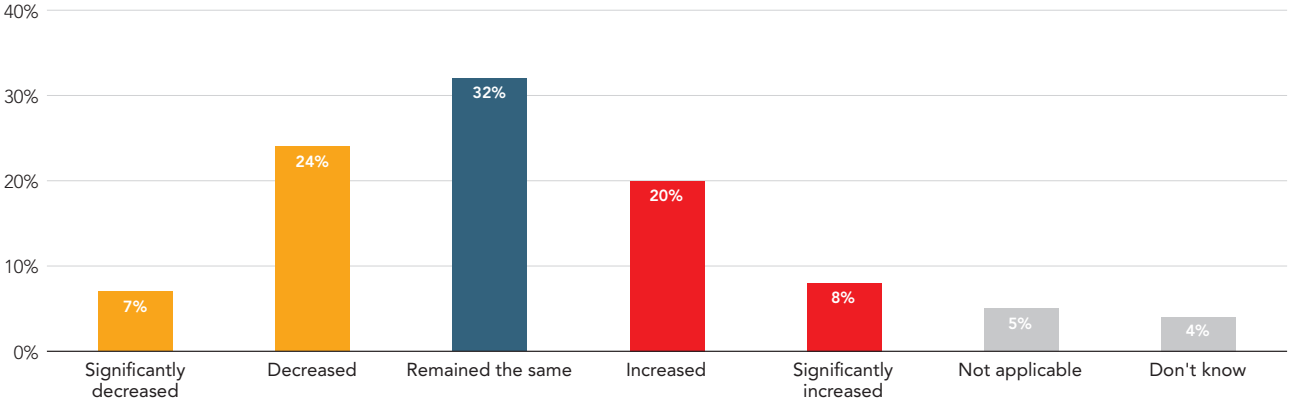


FIGURE 2.13: How would you evaluate the impact of remote / hybrid working on the effectiveness of the internal controls? (n = 1,956)



Working from home has heightened the risk profile for many entities around the loss of intellectual property. Studies show an increase in the range of phishing attacks, for example, since the start of the pandemic. VentureBeat references a study by SonicWall suggesting a 231% increase in phishing attacks since the start of the pandemic to the end of 2021 (Alspach 2022). Cyber protection has been moving towards a Zero Trust model (as discussed in ACCA / Chartered Accountants Australia and New Zealand / Macquarie University 2019) which defines the perimeter of the cyber threat in a different manner. The use of techniques such as the Zero Trust Model helps to redefine the risk profile.

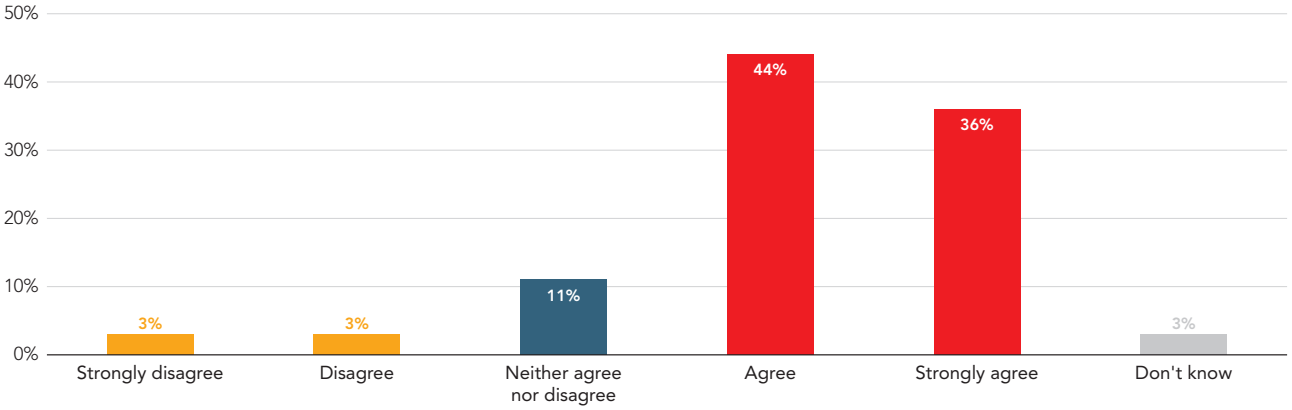
2.5 Non-financial reporting

The final consideration in the survey was whether the respondents believed that the internal controls should be extended to non-financial information, and reporting related to the ESG objectives (Figure 2.14).

Overall, 80% of the respondents either agreed or strongly agreed with this statement. This result showed only marginal regional variation.

In February 2022, the COSO Board approved a research study to demonstrate how effective internal control over sustainability reporting can be achieved by applying the 2013 Internal Control Integrated Framework.[10] It is very important that for investors and other stakeholders that there be trust and confidence in ESG/sustainability disclosures such as those on climate risk, carbon emissions, cybersecurity, innovation, and human capital. This data, reporting and analysis is different from financial data in that it tends to be more unstructured, qualitative, and estimated from different sources. Data governance, quality, modelling, and analytics are critically important.

FIGURE 2.14: To what extent do you agree or disagree that there is a need to apply the internal control framework to non-financial and ESG reporting? (n = 1,956)



OVERALL, 80% OF THE RESPONDENTS EITHER AGREED OR STRONGLY AGREED THAT THERE IS A NEED TO APPLY THE INTERNAL CONTROL FRAMEWORK TO NON-FINANCIAL AND ESG REPORTING.

10 COSO (2022)

UNLESS WE MODIFY OUR APPROACH ON IDENTIFICATION OF RISKS AND METHODOLOGY FROM AN INTERNAL CONTROL STANDPOINT, I DON'T THINK THE TRADITIONAL APPROACHES ARE GOING TO BE RELEVANT ANY LONGER.

3. Evolving our thinking

> **'CHANGE IS COMING AT A GREATER VELOCITY AND WITH MORE SIGNIFICANT IMPACT NOW THAN EVER BEFORE. THE TECHNOLOGY WE ARE USING AND THE RISKS AND REQUIREMENTS THEY FACE, PARTICULARLY FROM REGULATORS, ARE ALL EXPANDING.'**
>
> INTERNAL AUDIT CONSULTANT SPEAKING AT UK AND REPUBLIC OF IRELAND ROUNDTABLE

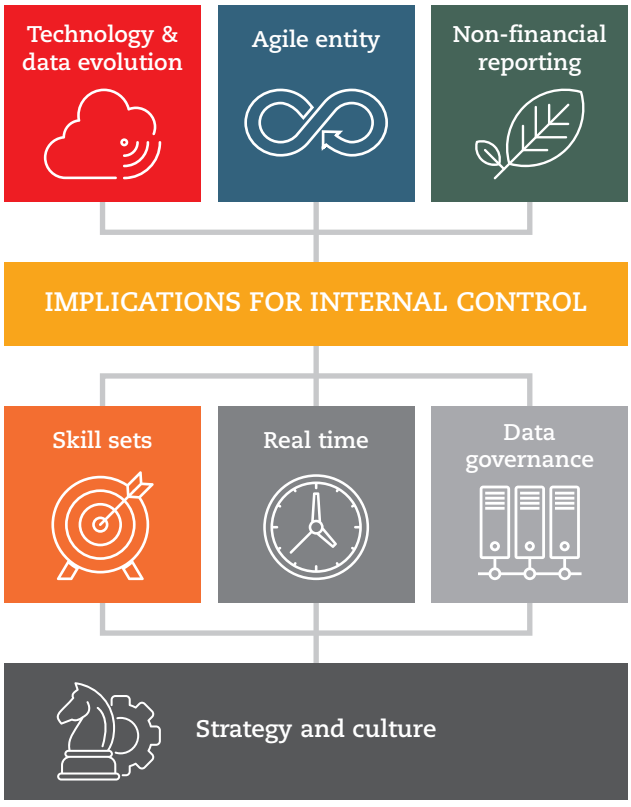
3.1 Charting a way forward

Having considered the current position through the survey results and appraised the perceptions of the interviewees and roundtable participants, it is important to chart a way forward for internal control, given the influences upon it. In this chapter several of the drivers are explored. Moving forward requires action to be taken – suggested action points are highlighted with an '**!**' icon.

The discussion is developed around several factors (Figure 3.1).

Understanding the risk profile is essential. Controls monitor risks and this link in the transformed entity remains essential (as discussed in section 3.9). The automation of controls, including the use of machine learning and other techniques, requires this to be in place. This, in turn, should integrate with the governance risk and compliance (GRC) platform that forms part of the overall technological architecture (see section 3.5).

FIGURE 3.1: Charting a way forward



3.2 Technology and data evolution

There is no escaping that technology and data are changing the business landscape. Before the pandemic, entities were increasingly focusing on understanding how to create value and insight from the data at their disposal, and on achieving these objectives. The view that the pandemic accelerated the rate of technology adoption was widely accepted by the roundtable participants and interviewees. The expression 'five years in five months' has frequently been used as a mantra for this technological acceleration. An accountancy firm partner in India commented that, 'like it or not, technology has dominated the business operations in the last …10 to 20 years. I would say more so in the last two years. The post-COVID impact of technology has been pretty stark and even where people were reluctant to embrace the change [they] were forced to [do so].' He added that in his view, 'unless we modify our approach on identification of risks and methodology from an internal control standpoint, I don't think the traditional approaches are going to be relevant any longer'. In the view of one US chief audit executive, 'what's happening in the audit world is [that] business processes are moving, but the audit function isn't moving as quickly'.

As has been shown from the survey results in Figure 2.13 the initial perception that the changed ways of working might result in a weakening of the internal control environment may not have come to pass. A CFO commented that for the first line: 'it's becoming quite difficult for one to understand the end-to-end process, and if you're failing to understand the process the second line or third line will normally have a challenge when they're trying to understand that process and then try and see if the controls are working properly or be able to undertake an audit of it'. In their view, the nature of processes is becoming more fragmented and informal. From the perspective of the first line it is more challenging to obtain the end-to-end view.

Among many of the roundtable participants there was a view that the informality of ways of working that the pandemic necessitated, for example by using informal methods to approve transactions, such as email approval or WhatsApp messaging, may have resulted in a loss of audit trail. One interviewee who works in a regulated industry accepted that while many of these societal changes are here to stay because lifestyle changes among the workforce have become accepted, it was now the time for entities to reappraise some of the new 'temporary' processes that were put into place quickly at the onset of the pandemic which have now become permanent and may need additional review. This interviewee continued that there was a balance to be struck, between the need for the control and the evolving work environment. There was a risk, in their view, that it was perceived that a control was only operating effectively when the individual was performing the task only when in the office, which might not be the case.

A chief audit executive based in the UK had a different perspective, commenting that: 'I don't think it is about more control. I think it is about more nimble control and [assessing] where we were probably over controlled. Our risk appetite was slightly out of whack'.

CONSIDER THE TECHNOLOGY AND DATA TRANSITIONS WHICH ENTITIES HAVE INTEGRATED INTO THE OPERATING MODEL AND ARE REFLECTING THESE IN THE INTERNAL CONTROLS.

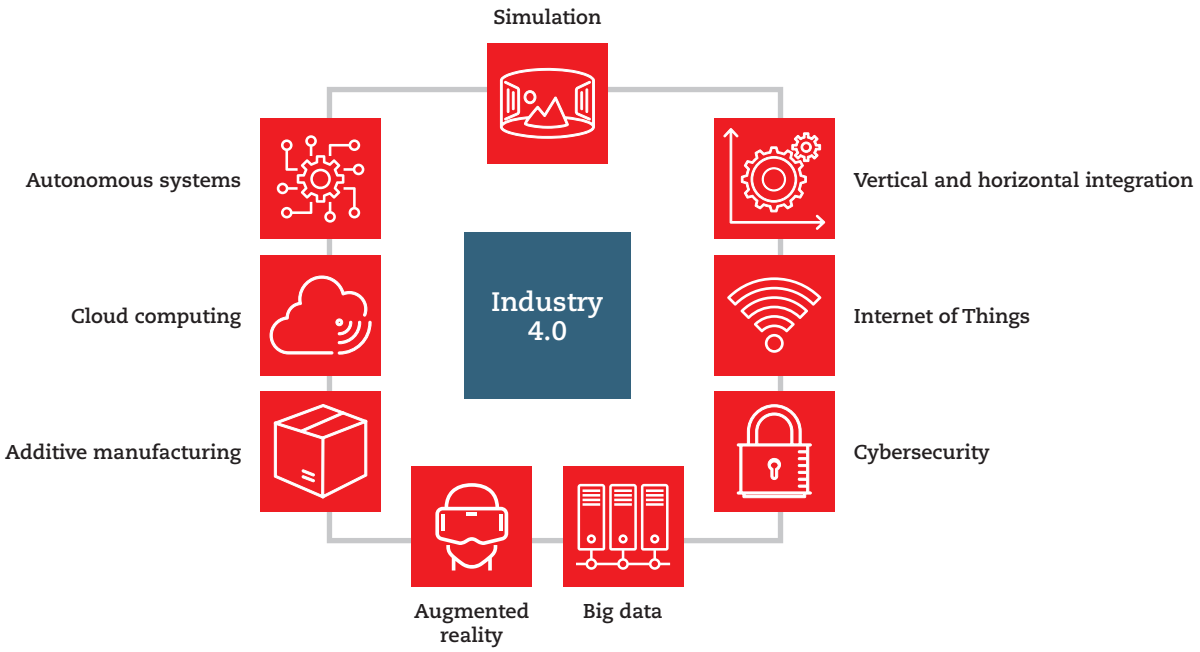
While there has been an acceleration of the pace of change in technology and data, this is unlikely to be the end of the story. The impact of the 'fourth industrial revolution' on entities is increasing, especially as they seek to address the economic climate that is emerging in 2022. An increased use of automation in the production cycle will affect not only manufacturing-based entities but those across all sectors in all areas of operations.[11]

The components of this revolution, termed 'Industry 4.0', are shown in Figure 3.2.

When considered in combination with the survey respondents' perceptions of technological impacts on internal control (Figure 2.10) would suggest that a reasonable proportion are not aware of the impacts of these technologies on their entities or the internal control implications. Standing still is not an option, nor is 'auditing around the box' (ie adopting new/unconventional approaches). Those involved in internal control need to be more aware of these technology and data drivers.

An Australian roundtable participant commented: 'the speed at which [technological change is] coming is increasingly faster than what we have seen before. The heavy technology reliance is also getting heavier and heavier as we go on. The challenge [is] for our internal control environment…to address that in whatever situation that we look at'. Relating this to the numbers of respondents who did not understand the impact of emerging technologies in relation to internal control, as the use of a range of technologies increases, so the potential gap widens.

FIGURE 3.2: Components of 'Industry 4.0'



11 As an example, the impact on Supply Chains of Industry 4.0 is considered in ACCA / IMA / Chartered Institute of Procurement and Supply (CIPS) (2022).

ENSURE THAT YOU UNDERSTAND THE TECHNOLOGY AND DATA DRIVERS IN THE OPERATING MODEL OF THE ENTITY. ENSURE THAT YOU ARE FAMILIAR WITH THE USE OF EMERGING TECHNOLOGIES.

MAP THE USE OF EMERGING TECHNOLOGIES TO INTERNAL CONTROLS AND IDENTIFY OPPORTUNITIES TO INCREASE CONTROL EFFECTIVENESS.

A South African roundtable participant took the discussion further. 'The fifth industrial revolution [will be] where humans and machines coexisting together gives us the opportunity to change the mindset, change the culture. We can use technology to ensure that we have operational efficiency'.

3.3 The agile entity

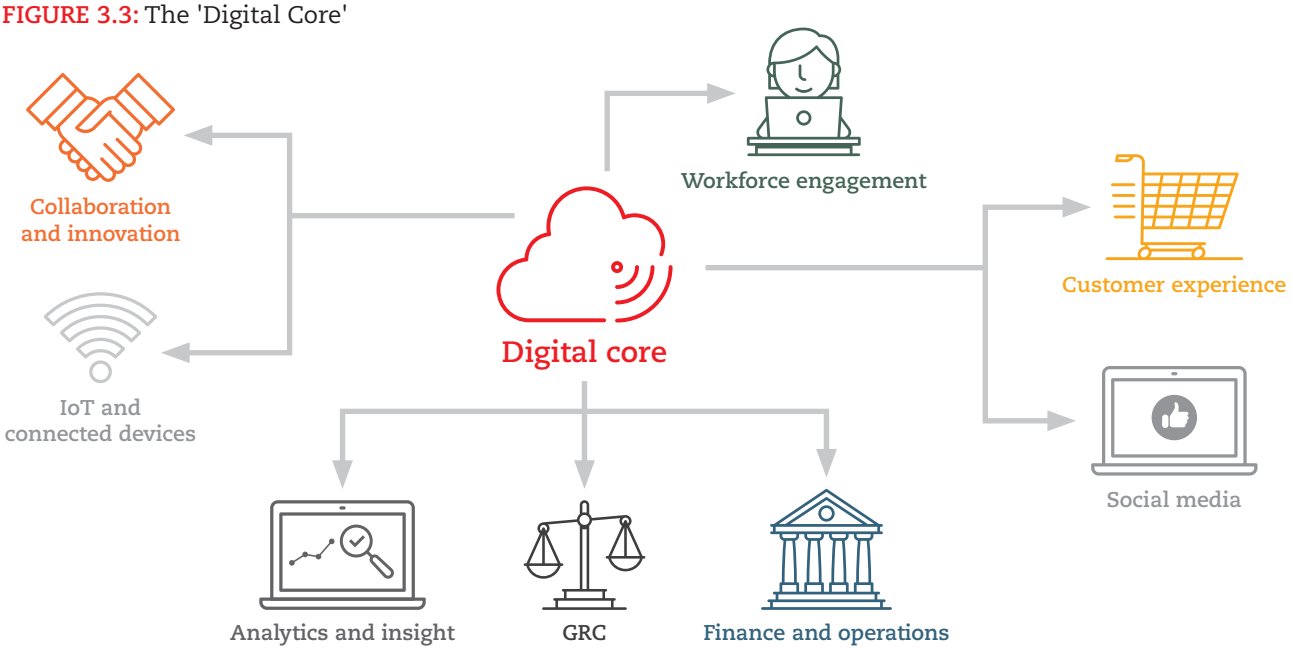
The economic drivers of 2022 and beyond are likely to mean that entities will need to be agile in adapting their operating models. Agility means that there is a need to constantly update and change the operating model to be able to exploit the opportunities and manage the constraints of the economic environment. This means that internal controls need to be adaptive and dynamic. The survey results suggest that internal control considerations remain a potential afterthought in the transformation process (Figure 2.7). As entities increasingly migrate to Cloud-based technology and data architectures built around 'best of breed' applications, the need to exploit this agility will increase. The concept of the 'Digital Core' (Figure 3.3) facilitates this rapid sense of change (see ACCA /CA ANZ/Generation CFO 2021).

It is important that those charged with internal control across all levels of operation within the Three Lines Model ensure that these considerations are included in the project teams that are responsible for driving these agile changes. Often these teams are assembled for short-term activities and stood down equally quickly. Making changes to accommodate internal control considerations as an afterthought is not possible, as was highlighted by several roundtable participants, and confirmed by their experiences. The mindset of those charged with internal control need to move from a 'waterfall' to an 'agile'[12] approach and to be proactive in establishing the case for involvement rather than waiting to be invited in.

APPRECIATE THAT OPERATING MODEL DEVELOPMENTS ARE EVER MORE LIKELY TO BE CONDUCTED IN AN AGILE MANNER AND ENSURE THAT THOSE CHARGED WITH INTERNAL CONTROL ACROSS ALL LEVELS WITHIN THE THREE LINES MODEL ARE PREPARED TO ENGAGE APPROPRIATELY.

As the breadth of internal control increases to include more non-financial as well as financial aspects of the entity, so there is a need for an integrated view of risk data. Although as McPherson et all point out, 'lead to risk data being fragmented, misaligned and scattered in

FIGURE 3.3: The 'Digital Core'



12 The terms 'waterfall' and 'agile' are defined in the Glossary.

organisational silos, which prevents leaders from gaining a necessary panoramic view of the risk landscape they need to act boldly and purposefully' (McPherson et al 2022). This progression of internal control requires the adoption of effective and efficient GRC solutions.

IMPLEMENT ONE GRC SOLUTION THAT ADDRESSES ALL ELEMENTS OF RISK AND INTERNAL CONTROL ACROSS THE ENTITY.

Several roundtable participants highlighted the challenges of data migration as entities transition to the digital core. While data migration can never be ignored, it is the inherent changes in the use of IT that this operating model introduces that must be appreciated. Cloud-based solutions require a different approach to application enhancement. Changes are released by the vendors according to their own timelines and operating models need to adapt. The traditional view of IT general controls does not apply. In the traditional technological operating models, entities competed in modifying the application to suit their own operating model. In the Cloud-based world, the operating models need to adapt to the model set by the vendor and the competitive landscape has changed, as entities compete to derive insights from available data. Internal controls need to be adapted to reflect this changing model, focusing upon the different operating risk profile. A CFO in the Middle East commented that: 'the biggest challenge is just because of technology evolving so fast: once you create a control, all of a sudden that control is no longer relevant and in some cases the controls are actually not commercially viable' noting that in his organisation there is no legislative or regulatory requirement for the implementation of such an environment.

RECONFIGURE THE RISK MODEL TO REFLECT THE CHANGED TECHNOLOGY PRACTICES THAT ARISE FROM THE ADOPTION OF CLOUD-BASED APPLICATIONS. UNDERSTAND THE DIFFERENT NATURE OF THE TECHNOLOGY AND OF THE VENDOR RELATIONSHIP.

While this approach may be relatively easy to adopt for larger entities, for those in the mid-tier, where internal control is equally important, adoption of new technology can be constrained by the availability of funds and a lack of technical capability to implement the necessary changes, in both the technology and internal control. This, of itself, is a barrier that these entities need to overcome, otherwise competitive advantage may be lost.

In July 2021 COSO published a guide, *Enterprise Risk Management for Cloud Computing* (Grob and Cheng 2021), which provides a perspective on this area. This extends the 17 principles (see section 1.1, Figure 1.2) to a Cloud-based scenario, provides a roadmap for implementing Cloud computing and describes appropriate roles and responsibilities.

The importance of SOC 2 reporting for Cloud-service providers was stressed by many roundtable participants.[13] Understanding what risks that entity needs to manage in interacting with a service provider is essential. One of the lessons learnt by entities in the 1990s during the initial round of IT outsourcing was that you cannot abrogate responsibility for risk, and indeed it takes as much effort to manage the relationship with the service provider as it did to run the IT operation internally. All that changes is the risk profile. The same message remains true today with the iteration of Cloud-based applications.

A chief audit executive in the US commented: '[entities traditionally] have their own set of controls around access management controls, their own governance controls and change management. And you're seeing [entities] including IT departments becoming more reliant on [the Cloud provider's] control framework. [As an auditor,] we are questioning is OK. We know this is a huge company and service, but how much are we going to rely on their framework, their controls and their structures and say that we're OK with that?'

APPRECIATE THE INTERNAL CONTROL CONSIDERATIONS ARISING FROM THE CHANGED RISK PROFILE IN ANY CLOUD-BASED SCENARIO. APPRECIATE THAT THE TRADITIONAL INFORMATION TECHNOLOGY GENERAL CONTROLS (ITCGS) HAVE CHANGED.

Cloud-based applications offer accessibility to the end-user, be that a customer or a staff member; vendor or supplier. Often, data capture is via a mobile device and occurs close to the time of transaction. Internal control that is framed by periodic detective reviews is too removed from the initiation of the transaction. The transaction is past. Using automated controls based on the mathematical parameters of the system or model provides more relevant feedback.

EMBED AUTOMATED AND PARAMETER-BASED INTERNAL CONTROLS INTO CLOUD-BASED APPLICATIONS, ESPECIALLY AT THE POINT OF INITIATION.

13 SOC 2 is AICPA's voluntary compliance standard for service organisations.

In February 2022 COSO released guidance on the application of agile methodologies to internal control (Walker 2022). The guidance outlines how an enterprise risk management (ERM) approach can be adopted in an agile business environment. The guidance makes 20 recommendations to strengthen ERM in an agile environment.

3.4 Non-financial reporting considerations

The reporting profile of entities is changing. Stakeholders are requiring a broader view of performance that includes ESG considerations; indeed, the range of these stakeholders themselves is increasing.

In March 2022 the US SEC published its draft *The Enhancement and Standardization of Climate-Related Disclosures for Investors* (SEC 2022), which in paragraph E comments 'As part of the registrant's financial statements, the financial statement metrics would be subject to audit by an independent registered public accounting firm and come within the scope of the registrant's internal control over financial reporting ("ICFR")'.[14]

The European Financial Reporting Advisory Group (EFRAG) has also published in March 2022 draft guidance on sustainability reporting which includes aspects of internal control (EFRAG 2022). Paragraph 43 suggests that 'the undertaking shall provide information on its internal control processes, including in relation to the sustainability reporting process'. Paragraph 44 provides a commentary by stating that 'the principle to be followed under this disclosure requirement is to inform about the aspects related to the governance factors that affect the undertaking's internal control processes, including in relation to sustainability reporting, and to provide an understanding of the supervision and monitoring of those processes by the undertaking's governance body'.

Also, in March 2022 the International Sustainability Standards Board (ISSB) published its exposure drafts on general sustainability-related disclosure requirements (ISSB 2022a) and specifying climate-related disclosure requirements (ISSB 2022b). Between them, these outline the proposed internal reporting standards in this area.

Irrespective of the outcome of these consultations, the scope of reporting and the required internal controls of larger entities will expand to include non-financial components. This was clearly expected by the survey respondents (Figure 2.14).

Many of the roundtable participants also addressed this area. For several, while they already expected to include non-financial data in their internal control environment, there was also a recognition that this presents challenges that entities will soon need to face.

Firstly, as roundtable participants and interviewees commented, many entities do not currently collect the full range of data that may be required by such disclosures. Many of the data components lie outside the entities themselves, in their supply chains. Obtaining and managing such data is clearly an issue that will need to be addressed.

Secondly, the applications are not yet in place to manage this data. While the software vendors may well develop new applications, much of the current reporting is developed using end-user-based applications, such as spreadsheets, which are already understood as weaknesses in internal control environments.

Thirdly, in contrast to financial reporting data, much of the required non-financial data is unstructured and qualitative in nature. This presents challenges in developing a level of internal control assurance over the data. As is discussed in section 3.8, there was a strong sentiment among the roundtable participants that there is a need to understand the ever-increasing alignment between data governance and internal control objectives. This area is a prime driver.

A chief audit executive from Central and Eastern Europe noted that: 'the [non-financial] data is obviously mostly located outside the ERP [enterprise resource planning] systems. It is collected in an ad hoc manner really, only when it is needed for reporting. You can imagine if [it has] to be compiled manually how hard it is to audit it. It is sort of creative work and sometimes I think it's just a rough approximation'.

WORK TO IDENTIFY THE RELEVANT DATA SOURCES TO ENABLE THE ENTITY TO MEET THE REQUIREMENTS OF NON-FINANCIAL DISCLOSURES.

DEVELOP A STRATEGY FOR INCLUDING THE NECESSARY NON-FINANCIAL DATA REQUIRED INTO THE INTERNAL CONTROL FRAMEWORK AND BE PREPARED TO DOCUMENT AS APPROPRIATE.

LIAISE WITH THOSE CHARGED WITH DATA GOVERNANCE TO ENSURE ALIGNMENT ACROSS THESE DATA SETS.

One interviewee with lengthy experience in internal control and who consults with many large corporates reflected upon whether those responsible across the IIA's Three Lines Model were ready to embrace non-financial reporting data streams within their objectives. His assessment was, 'No. Not of as of now at least'.[15]

14 SEC (2022) section E p; 43; referencing section II F 2 and 3 within the same document.

15 In February 2022 the COSO board approved a study on Sustainability / ESG (COSO 2022) with a view to publishing its results later in the year.

3.5 Details of the implications for internal control

Each of the trends outlined in the sections above has an implication for the internal control environment in an entity. These implications will continue to extend, and the reality of the changing environment is one that entities need to ensure that they address. This section considers some of the implications in more detail and considers several technological and data implications for finance (Figure 3.4).

Around or through

A classic question of auditing is whether to audit around or through the computer.[16] Do you treat the computer algorithm as a black box? Entities' substantial reliance upon IT means that attempts to audit 'around' the computer do not reflect how the entity operates. There is a potential misalignment of risk profiles. Some of the discussion in the roundtables reflected that, for many internal audit teams, there was still a tendency to audit 'around' the computer, owing simply to a lack of skills (see section 3.6) or to expediency. There was a sentiment in many of the discussions that entities relied upon manual controls and had many duplicative manual processes that formed part of the internal control framework as this was easier than understanding and implementing automated controls. As one interviewee commented, it is easier to document and prove a manual control than an automated one.

Yet for several roundtable participants there was an acceptance that if entities are to successfully manage the ever-increasing volumes of data that their entities either originate or need to be managing[17] then automated controls are essential. One India-based interviewee commented: 'You check one sample in an automated control, and you're done. Because if it works at a point in time, it's supposed to work always [assuming that the coding is correct]. And you could have five samples. We have to move towards automated controls'.

A UK-based CFO highlighted a dichotomy. 'We have sort of become more trusting or had to become more trusting of our folks, and that is also a dichotomy with internal control, because in one way, internal control says, "I don't trust you enough therefore I want to protect you and I need to involve more people in this process", and I think that that might need some thinking through'.

A Republic of Ireland contributor commented, 'people do not understand how to document those automated controls or [know] that…automated controls can save a lot of time and can …get into a lot of more of the risks of the system rather than going back to the ticking and bashing and the manual controls'.

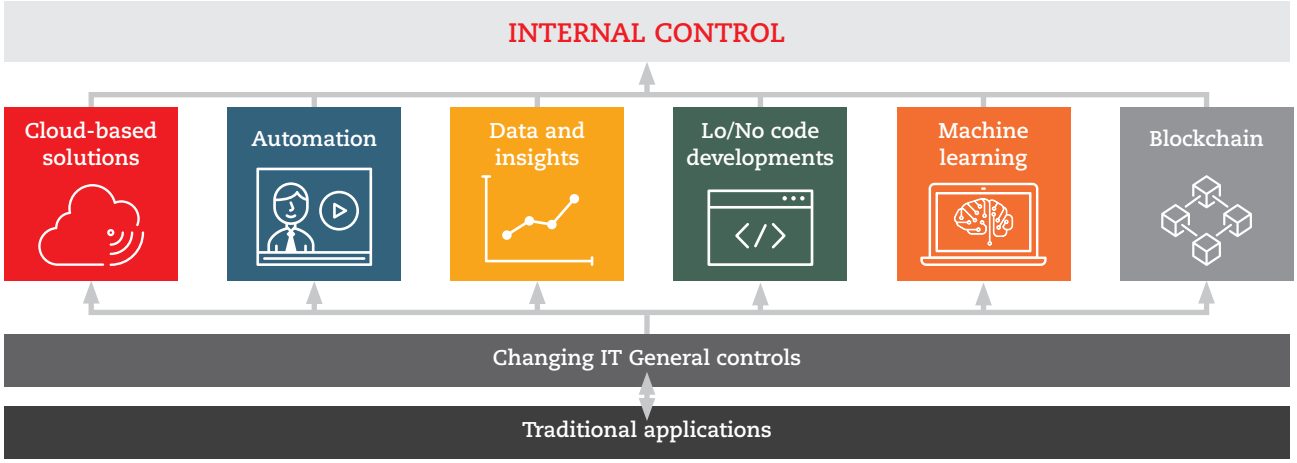
A European chief audit executive cautioned that, as entities move towards global processes and standard controls, there may be challenges in understanding how these are applied in specific locations. This participant added, 'finding…the common denominator that could be used for an automated control in terms of one size fits all is difficult'.

RE-EVALUATE THE APPROACH TO AUTOMATED CONTROLS WITHIN THE ENTITY.

IDENTIFY AREAS WHERE MANUAL CONTROLS ARE UNDERTAKEN THAT MAY DUPLICATE AUTOMATED CONTROLS AND ELIMINATE AS APPROPRIATE.

The use of automated controls may involve an element of continuous monitoring (as discussed in section 3.7).

FIGURE 3.4: Technologies affecting finance and internal control



16 The reference to the term 'computer' is to infer the totality of the applications and hardware.

17 An example of where an entity may increasingly need to process and validate information on other entities relates to their ability to address proposed European Union supply chain disclosures, as discussed in ACCA / IMA / CIPS (2022).

Changing working environment

Entities are still grappling with the workplace changes that have resulted from the pandemic. Even before COVID-19, the traditional business model based on physical presence was being replaced by one based upon contribution to the entity, and this trend has accelerated. In many entities, time and location are no longer issues, value and efficiency are the key drivers. Collaboration is the order of the day if entities are to survive in turbulent times. Several of the roundtable participants questioned whether internal controls based upon manual procedures or physical presence can be deemed effective for the future. Some roundtable participants who represented the internal audit community commented that, in their reviews of processes and controls, they had reverted to more substantive procedures to compensate for some of the informality introduced in remote work.

A CFO who contributed to this report considered these implications together with those of the challenging economic environment of 2022, noting that as entities' costs [and profits] become more squeezed and ways of working more informal: 'you find that you have challenges of even basic things like segregation of duties. When someone goes on leave it just becomes a very difficult challenge. Then you find that controls might be breached'.

Another CFO commented on worries about the dispersal of data via email. As phishing emails become more sophisticated, so the risks increase.

Data integrity and confidentiality are no longer functions of physical controls, for example being in an office and connected to a network, rather they are logical controls of authentication, virtual private networks, and encryption. Some of our bases of confidentiality have changed.

As ways of working change, so we need to reappraise the fundamentals of internal control from the perception of staff being physically present to a more value-driven acceptance of how roles are performed. Many traditional (and perhaps more manual) controls are now no longer effective. Automation is a necessity.

End-user developments and the use of Lo-code / No-code solutions

The traditional end-user computing tool was the spreadsheet. Studies, such as one conducted by ACCA (2020), indicate that as accountancy and finance professionals we continue to rely upon spreadsheets and are slow to embrace further forms of analytical or process efficiency tools, such as analytics tools and RPA (ACCA et al. 2018) or (Jiles 2020). Each of these is essentially an end-user-developed solution. As one chief audit executive commented, these end-user-developed solutions need to be subject to the same level of development controls as more traditional end-user computing applications. Yet, for entities to be agile they need increasingly to adopt and not avoid these solutions.

UNDERSTAND THE SCOPE OF END-USER COMPUTING (INCLUDING THOSE OUTSIDE THE TRADITIONAL DEFINITION) AND ENSURE THAT ALL APPLICATIONS THAT ARE DEVELOPED AND THAT FORM PART OF THE INTERNAL CONTROLS, HAVE THE APPROPRIATE LEVEL OF DEVELOPMENTAL AND TEST CONTROLS APPLIED TO THEM.

This is but one stage in the journey. The agile entity will increasingly use solutions that can be rapidly developed and deployed often using either No-code or Lo-code development tools to enhance the operating model. These solutions are used by the end-user rather than by the IT department and can be developed and deployed rapidly. There is a risk of a lack of formal recognition of the internal control considerations in such scenarios, yet they form a fundamental part of entities' operating models, using the Cloud-based environment to the full.

APPRECIATE THAT AGILE TRANSFORMATION WILL INCREASINGLY USE APPLICATIONS TO DEVELOP ENHANCEMENTS TO OPERATING PROCESSES THAT ARE NOT SUBJECT TO TRADITIONAL APPLICATION DEVELOPMENT LIFE CYCLES AND ENSURE THAT THE RISK ARISING IS ADDRESSED.

Even in the application of technologies the tendency is to view these through a process lens and not to look at the control opportunities that they can present. As one India-based interviewee commented, for every process to which we apply RPA, it is possible to consider a parallel control-based method. They considered that there was insufficient emphasis being placed on the use of RPA for internal control purposes.

IT general controls

The traditional view of IT general controls (ITCGs) is that they apply to all computer systems and the environment in which they operate. There are several sources of guidance in this area.

- IIA has released a series of Global Technology Audit Guides that support the understanding of several areas that are relevant to the audit of this environment.
- The Information Systems Audit and Control Association (ISACA) has published its Control Objectives for Information Technology (COBIT) framework, which aligns technology objectives to the COSO framework.
- AXELOS, which is jointly owned by Capita and the UK government's Cabinet Office, has a set of IT-related standards known as the IT Infrastructure Library (ITIL).

Each of these forms of guidance is regularly reviewed and updated. Even so, the traditional view of ITGCs, expressed by the roundtable participants, is that they are applicable to the legacy computer environment. With the advance of 'as-a-service' technologies, the ways in which entities consume and use IT services is changing. This supports the development of the agile and transformative entity. When developing internal controls, it is important to understand how the IT environment is changing. As one North America roundtable participant commented, in his company, 'it is almost laughable that…we apply the same IT general controls methodology that we did 20 or 30 years ago'.

As commentator Matt Kelly points out: 'ITGCs work out of sight from most employees, but they're incredibly important for security, compliance, and operational success. The one overriding fact, however, is that the modern business enterprise will only rely more on technology as we move into the future. The stronger your grasp over the ITGCs that support your business, the better your business will be able to compete in our highly regulated, highly risky world' (Kelly 2022).

EVALUATE THE IT GENERAL CONTROL ENVIRONMENT IN THE CONTEXT OF THE CURRENT OPERATING MODEL, IDENTIFYING WHERE CONTROLS ARE MANAGED THROUGH CLOUD-BASED RATHER THAN ON-PREMISES APPLICATIONS AND THE RESULTING CHANGES IN THE RISK PROFILES.

Blockchain

Blockchain technologies are often cited as environments where control objectives are integral to their fabric. To date, use of this technology has been limited to certain circumstances, such as those where the provenance of goods or financial data is of critical importance. As provenance becomes an increasing entity-level risk, for example to assist in addressing ESG objectives, so the use of this and similar technologies is likely to increase. Appreciating how this technology can assist in addressing precisely defined control objectives is important for entities.

In July 2020 COSO published guidance on the application of internal control in a blockchain scenario (Burns et al. 2020), in which the authors assess the potential impact of blockchain on internal control.

Machine learning and artificial intelligence

Inspection of data increasingly requires the detection of patterns learned from experience. This is not the only case for the use of machine learning (ML) and artificial intelligence (AI) in entities. As control techniques, these present challenges given that, as the algorithms learn during use, it becomes challenging to understand whether true or false positives are being detected in data sets, or to develop more focused projections. It requires a deep skill, such as those of an algorithm auditor, to evaluate their effectiveness. Yet many planning and forecasting cycles that lie at the heart of management review controls are using elements of ML to improve the accuracy of their forecasts.

For those responsible for internal controls, in whichever part of the entity, one of the fundamental ITGCs, change management, needs to be applied in a different sense to the algorithm. In the traditional environment, changes were documented and appraised. ML does not create such an audit trail. It learns as it proceeds. The potential of bias in algorithms is well understood – yet it is not possible to apply conventional change management procedures. There is a temptation to treat the algorithm as a 'black box', yet even that requires skilled analyses of expected against actual outcomes. But ML is here, and it is important to upskill accordingly.

APPRECIATE THE ROLE THAT MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE CAN PLAY IN THE CONTROL ENVIRONMENT.

All these detailed trends have implications for the skill sets of those in each of the three lines.

In September 2021, COSO published guidance on ML and relates the COSO framework to its use (Calagna et al. 2021). The guidance maps the 17 principles to their applicability to AI and its potential uses in entities.

3.6 Skill sets

The question of which skills should be developed to remain relevant as an accountancy and finance, internal audit or other practitioners is one that is frequently raised. Charlie Wright, the IIA chair of the Global Board 2021–2022, in a discussion of the future skills of the internal auditor made the following comment.

> 'Despite this potential, only 38% of chief audit executives or heads of internal audit participating in an October 2020 global study [conducted by IIA and Deloitte] exploring internal audit competency said they felt their functions had the capability to audit more than three of six critical areas related to technology and innovation. These areas included:
>
> - disruptive technologies
> - Cloud and virtual computing environments
> - extended ERM
> - cybersecurity
> - dynamic risk assessment
> - business continuity and crisis management.'
>
> Source: Wright 2021

There is a clear need to develop a broad range of skills both technical and more inter-personal in nature.

Separate studies by ACCA (2020 and 2021) and IMA (Krumwiede 2017) concur with this analysis for all accountancy and finance professionals. Upskilling can be achieved only through continuous learning but this is not just learning technical skills: the accountancy, finance and internal audit professional also needs to be a trusted adviser.[18]

As internal control continues to transform, so the skill sets of those charged with it need to expand. An appreciation of technology and data are no longer 'nice to have', rather, they are necessities. The challenge of this statement can be seen reflected in the survey results referenced in Figure 1.4 and in Figure 2.7, which indicate the level of the skill shortage and its impact on project-related work.

IDENTIFY THE SKILL SETS AND RESOURCES NEEDED TO SUSTAIN THE EFFECTIVENESS OF INTERNAL CONTROL ACROSS THE TRANSFORMED ENTITY, INCLUDING SKILLS NEEDED TO ADDRESS NON-FINANCIAL OBJECTIVES. DEVELOP APPROPRIATE TALENT-MANAGEMENT PLANS.

CONSIDER YOUR OWN LEVEL OF TECHNOLOGY AND DATA-RELATED SKILLS IN THE CONTEXT OF INTERNAL CONTROL AND IDENTIFY RELEVANT DEVELOPMENTAL OPPORTUNITIES.

APPRECIATE THAT SKILLS NEED TO BE REFRESHED ON A CONTINUAL BASIS, BOTH IN TECHNOLOGY AND IN BUSINESS ACUMEN AND INTERPERSONAL SKILLS. ENSURE THAT RELEVANT INITIATIVES ARE IN PLACE.

The importance of Big Data and the transformation process requires that each line of the Three Line Model needs to ensure that staff have the appropriate skill sets to manage the risks. At a time when, for many entities, resources are constrained for several reasons, this presents a significant challenge, but one that cannot be ignored.

A chief audit executive working in a global multinational company in India commented that there is level of expectation in relation to the skills needed to support data analytics and queries, opining that spreadsheeting skills are no longer sufficient. 'There is now a certain amount of basic coding [that] we would expect. At least, each team member needs to be able to apply [a] certain basic level of coding themselves, then go to a specialist, because you're still not called a specialist. This is the new reality of today and tomorrow that you need to have these basics. These skill sets [are] no longer specialist'. This participant pointed out that coding skills are now as necessary as Excel skills have been in the past.

A CFO reflected upon the impact of automation on process flows and the skill sets that will be needed for an effective internal control environment in the future. 'You have a skill mismatch where you have improved the efficiencies generally in lower-grade jobs, releasing capacity, but the skills you need are in higher-grade jobs. You have created space, but there is a mismatch of skills, which I think is a challenge for us in the way we approach control'.

One interviewee suggested the following model to describe the skill set needed in an entity from an internal control perspective (Figure 3.5).

As Figure 3.5 implies, the technical skills are no longer sufficient on their own. In a transforming environment having a robust operational knowledge of the entity and its industry is key, as are the interpersonal skills to be able to communicate this knowledge effectively and thereby establish trusted relationships with stakeholders at all levels.

FIGURE 3.5: A potential skill set model in the internal control context

18 A concept developed by Maister et al. in their 2002 book, *The Trusted Advisor*, since updated (Maister et al. 2021).

3.7 Real-time data considerations

The ability to review large volumes of transactions in real time can be a necessity for many entities but is challenging as the volumes of data increase and the potential risk profile broadens. Internal control has traditionally been a reactive activity. It reviews transactions in each line of the Three Line Model, either as they happen or at a point in time after they occurred. With the increasing velocity and veracity of transactions, for many roundtable participants and interviewees this had become increasingly challenging. For some, especially in the third line, providing observations on transactions that were long past seemed to raise questions about their relevance to the entity.

The potential of using data inspection techniques such as embedded code to identify potential patterns in transactions in real time offers an opportunity not only to make the performance of a control more proactive but also to increase the value added to entities.

For entities that exist in a fast-moving operating environment, change is a constant. Business processes are constantly being refined and adapted. For many entities, the traditional cycle of periodic operational and process change has been replaced with continuous change. The challenge for those responsible for internal control is that any retrospective review may be irrelevant, as the process may have changed since the data was gathered.

It is important to strike a balance between the continuous monitoring of data and the identification of transactions that might require further investigation, with the assessment of strategic risks and subsequent audit work. Separating these two channels of the second and third lines may become essential. Some of the roundtable participants commented that continuous monitoring is a second line activity. It is only effective, however, if action is taken once a red flag has been raised. The third line must consider how effective the follow-up procedures are.

An interviewee based in India reflected upon the challenge of small sample or selection sizes in relation to the large volumes of data held by entities. 'The coverage and the variations that exist [make it challenging] for you to conclude that internal controls are appropriate and are designed appropriately. How do you come to that conclusion with such a little sample size, which is what is advocated in many of the guidance notes? I think that's where the importance of analytics comes into play. That gives you wider coverage, and [in] a far more scientific [as opposed to a selection] and focused manner'.

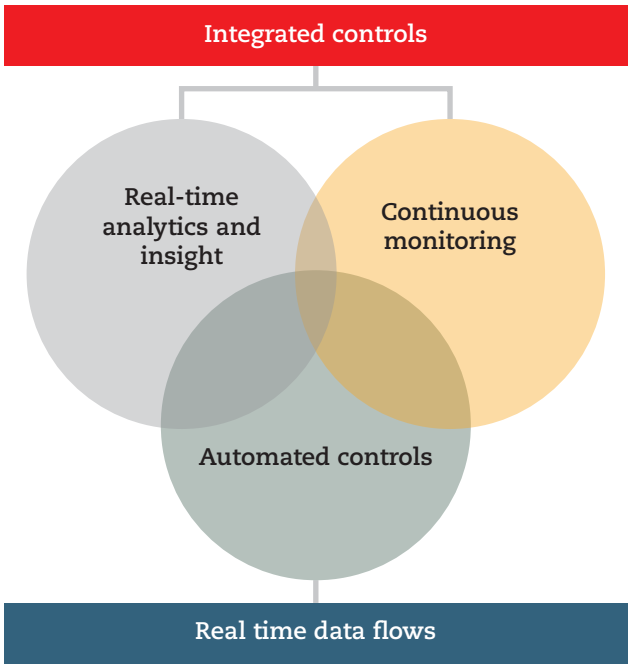
The efficient automation of controls depends upon several factors:

- an understanding of the capabilities of the application to validate transactions as part of the workflow
- building into that workflow the appropriate levels of oversight
- using reports to monitor the performance of the process, identify trends and isolate outliers for investigation
- using the workflow intelligently to document the control activities
- using bespoke developments and end-user tools, such as RPA, to develop monitoring controls.

Several roundtable participants highlighted a lack of robust evidence as a barrier to automation.

The integration of continuous monitoring and automated controls within the overall internal control structure is essential if entities are to manage the increased volumes of data effectively in a transformed operating environment. Figure 3.6 provides a view which links the components of automated controls (at the data validation level), real-time analytics and insight (monitoring performance at the business level) and continuous monitoring (providing attestation). The combination of these three techniques will be essential for an integrated control schema in the entities of the future.

FIGURE 3.6: Role of continuous monitoring and real-time analytics



DEVELOP AND ENACT A STRATEGY FOR CONTINUOUS MONITORING THAT IS ALIGNED TO THE EXPECTED DATA VOLUME.

ENSURE THAT THERE IS AN APPROPRIATE BALANCE OF MANUAL AND AUTOMATED CONTROLS AND SEEK TO AVOID REDUNDANCY AND DUPLICATION IN CONTROLS.

3.8 Data governance – a question of internal control?

If internal control is to broaden in its scope to embrace data that is used for both financial and non-financial performance and reporting objectives, then the integrity of that data becomes ever more important. Nonetheless, from a different perspective, this is also the objective of those charged with data governance. A chief audit executive from the US who participated in the North America roundtable commented: 'data governance is a real issue and until you have proper data governance, all the frameworks, all the controls or the principles that any internal control framework talks about…will not be relevant'.

A UK roundtable participant commented that the: 'technology backbone that has consistent data or consistent data structures capable of providing measurement of [the strategic] outcomes [is necessary]. So, what Boards and audit committees want to know is, where are we on that journey to delivering those outcomes? What is getting in the way of that? What are the risks and what sort of control environment [do we need] if we are to manage and mitigate that in the most economical, efficient and effective way?'.

Table 3.1 provides a comparison of internal control and data governance objectives in entities. It demonstrates significant areas of common interest.

For many roundtable participants, a closer alignment between those charged with delivering the internal control objectives and those ensuring data governance in an entity was essential for the future.

While those responsible for data governance are accountable to management for the integrity of the data flows, those charged with internal control (and internal audit) are accountable to groups such as the audit committee. Both have common interests in the completeness and accuracy of data, and as the requirements for internal control increase across non-financial as well as financial data, so the areas of common interest will increasingly overlap.

ENSURE ALIGNMENT BETWEEN THE DATA GOVERNANCE AND INTERNAL CONTROL OBJECTIVES IN THE ENTITY AND STRENGTHEN PROCEDURES ENSURING THE COMPLETENESS AND ACCURACY OF BOTH FINANCIAL AND NON-FINANCIAL DATA.

3.9 A question of strategy and culture

The final consideration for many of the roundtable participants was the alignment of internal control with the strategy of the entity and with its culture. This can be captured in the 2017 COSO Enterprise Risk Management (ERM) framework (Figure 3.7).

TABLE 3.1: Internal control vs. data governance principles

INTERNAL CONTROL PRINCIPLES	DATA GOVERNANCE PRINCIPLES
■ Establish responsibilities ■ Maintain records ■ Insure assets by bonding key employees ■ Segregate duties ■ Mandatory employee rotation ■ Split related-party responsibility ■ Use technological controls ■ Perform regular independent reviews	■ Ensure accountability ■ Apply standard rules and regulations ■ Ensure data stewardship ■ Establish data quality standards ■ Ensure transparency

FIGURE 3.7: COSO Enterprise Risk Management Framework

Source: COSO (2017)

Several expressed the opinion that internal control activities were being undertaken for the sake of compliance rather than because there was a specific risk that was being controlled. They argued that a balance needed to be achieved. One chief audit executive based in the UK provided a slightly different perspective, commenting that: '[as] control functions we forget [the] risk appetite element of control, and it's "belt and braces" all the time, and I think the pandemic has helped us get a little bit more perspective on that'.

There was a sense that the gap between controlling real risks and compliance activities was increasing in line with the increase in data flows and the implementation of technology. If manual controls are repeated by automated controls, then this duplication reduces the effectiveness of the control environment overall. Control needs to be cost effective.

An internal control framework exists to 'to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance' (COSO 2013). Implicit in this is the link to the management of risk. That can only be achieved by a strong culture of risk management and a reinforcement of the purpose of internal control. This culture must be established by the entity's senior leaders. Some roundtable participants argued that this link was weakening. The importance of effective enterprise risk management and its strong link to internal control objectives was highlighted by many. One chief audit executive from the UK commented: 'People generally have a view that controls make things more difficult and for me…one of the challenges that I think we have to face as professionals in our discipline is to actually try and change that culture and encourage people… [to understand] that controls actually help them'.

Participants reported an increasing suspicion of the purpose of internal control among those generations now entering the workplace. Their level of technological literacy and their familiarity with technology were an essential part of their lives, and their belief that 'the computer is always right' was deemed to risk a potential weakening of internal control. If internal control is to be effective, it needs to be understood that it requires a combination of people, process, technology and data. If even one of these components is not effective, then the effectiveness of the internal control framework is reduced.

An Australian roundtable participant commented: 'I think in the digital age with data governance and internal controls, culture will be more important as controls become really embedded in automated systems and technology'.

Several roundtable participants and interviewees contrasted the cultural attitudes to internal control with their impact on entities. In part, this can be seen in the variations in responses to the survey, especially when correlated with the lack of board oversight (Figure 1.4) where views differ between Western Europe and North America on the one hand and those in the Middle East, South Asia and Asia–Pacific. This can also be attributed to different perceptions of regulation and variations in ownership structures.

REINFORCE THE IMPORTANCE OF RISK MANAGEMENT AND INTERNAL CONTROL ON A CONTINUAL BASIS ACROSS THE ENTITY.

REINFORCE THE NEED TO BE OPTIMAL IN DEVELOPING AND IMPLEMENTING AN INTERNAL CONTROL FRAMEWORK, ESPECIALLY AS IT IS INCREASINGLY TECHNOLOGY ENABLED.

CHALLENGE THE ASSUMPTION THAT THE 'COMPUTER IS RIGHT' IN ALL CIRCUMSTANCES WHEN CONSIDERING INTERNAL CONTROLS.

3.10 Implications for internal control frameworks

In this discussion of the future considerations for internal control, it is important to reflect upon the frameworks that we use as a basis for establishing the control environment.

Figure 3.8 shows that the survey respondents were generally (62%) in either agreement or strong agreement that the current regulatory guidance reflected the nature of their operating model.

An analysis of the responses from those who either agree or strongly agree to this proposition shows some variation by region (Figure 3.9).

Many of the roundtable participants and interviewees concurred with this perspective. The core frameworks that they referred to, such as the COSO Internal Control – Integrated Framework, the Control Objectives for Information Technology (COBIT®) developed by the ISACA, and the SOC 2 framework developed by the AICPA.

As has been shown in this report, it is at the practical level that individuals are challenged. A participant on the US and Canada roundtable asked: '[do people think] the COSO Internal Control framework needs to be completely blown up and redone? It doesn't. I think the biggest deficiency that I see [in relation] to frameworks is [that] the practical application to [possibly] more complex areas [is] really falling behind'. An Australian roundtable participant commented that: 'the controls are implemented via procedures, which are promulgated in an [entity]. These days, most of the procedures live inside electronic boxes and with the cost of modifying computer systems, the internal procedures are not going to change very much inside computer systems so the business can move on. The procedures that might well have been right when they were written, never change. That can be a significant problem [for the entity]'.

There is an appreciation of the need to embrace digitalisation and transformation, but a lack of understanding of how to do this was cited as a barrier. Any guidance will, inevitably, be generic and while it can provide an element of support it cannot provide the specific context in which an accountancy and finance professional, wherever operating at which ever line will need to apply it. That must come, in part, from an appreciation of the technologies themselves and the management of the data.

FIGURE 3.8: To what extent do you agree or disagree that the regulatory guidance on internal control reflects the nature of the current operating model? (n = 1,956)

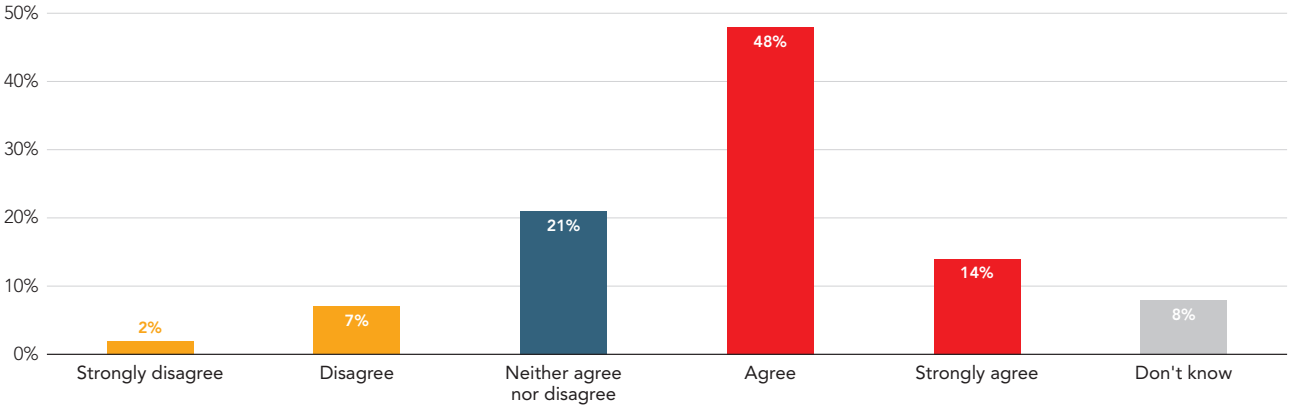
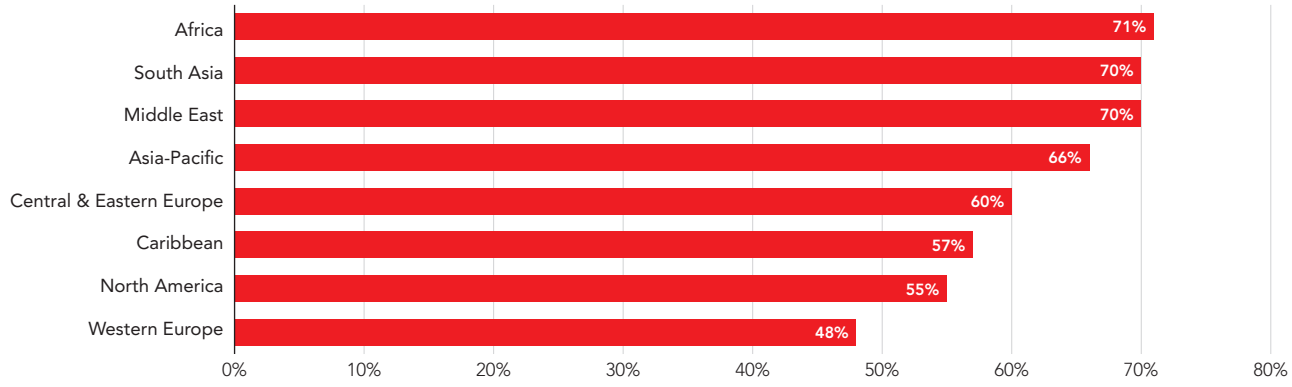
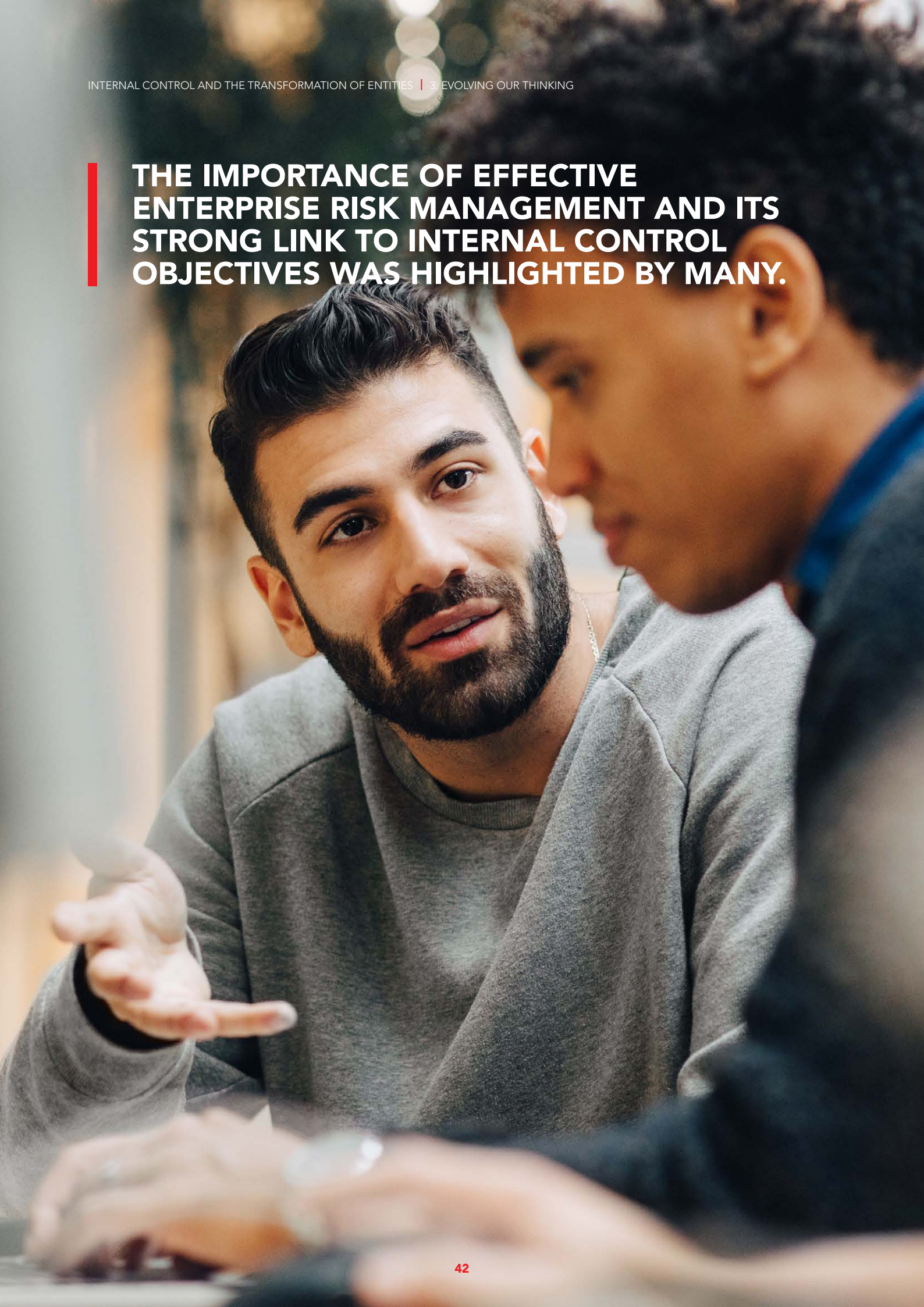


FIGURE 3.9: To what extent do you agree or disagree that the regulatory guidance on internal control reflects the nature of the current operating model? Analysis by region of Agree and Strongly Agree responses. (n=1,950)



THE IMPORTANCE OF EFFECTIVE ENTERPRISE RISK MANAGEMENT AND ITS STRONG LINK TO INTERNAL CONTROL OBJECTIVES WAS HIGHLIGHTED BY MANY.



Conclusion

Internal control remains a fundamental concept for entities and those responsible for governance. Stakeholders are increasingly looking for **assurance** over a broader range of disclosures from entities, which in turn requires the extension of the internal control framework across more process flows, some of which have not previously be within the scope of the IIA's Three Lines Model.

The availability of the right **skills** is fundamental to the maintenance of effective internal controls. These skills are broadening beyond the purely financial and there must be recognition of this expanded need and the consequent investment required both by entities and individuals.

Technology continues to advance. This advancement shows signs of accelerating as data and the applications and processes to support it become essential in the agile business environment. Internal control needs to be a fundamental part of this **transformation**; not an afterthought that is compensated by manual controls. Entities operate in **real time**; so, controls must operate through approaches such as continuous monitoring to keep pace with the activities of the entities operating them.

If entities are to integrate **non-financial reporting** objectives into their internal controls, there must be recognition that the data for this is less robust and more varied in its nature and its sources than financial data.

Technology is needed as well as strong data management and a close link to **data governance** objectives.

To support all these aspects of transformation, and to continue to have effective internal controls, more relevant guidance is needed to support practitioners and continuing education initiatives are necessary to develop the requisite skills. This applies not only to the use of the transformative technologies themselves, but also to our understanding of the IT control environment that supports them.

The bottom line is that the value of internal control extends well beyond statutory reporting and compliance to supporting external financial disclosures. In a fast-changing and expanding business environment (including drivers such as technological developments and ESG), effective internal control helps to build confidence, trust and reputation. In addition, to support business transformation and increase enterprise value, internal control itself must constantly transform to be fit for purpose in a digital and disruptive environment, and this requires training and upskilling. This is a great opportunity for accountancy, finance, and internal audit professionals to increase their relevance and influence.

TO SUPPORT BUSINESS TRANSFORMATION AND INCREASE ENTERPRISE VALUE, INTERNAL CONTROL ITSELF MUST CONSTANTLY TRANSFORM TO BE FIT FOR PURPOSE IN A DIGITAL AND DISRUPTIVE ENVIRONMENT, AND THIS REQUIRES TRAINING AND UPSKILLING.

Glossary

Additive manufacturing (AM)	AM, or additive layer manufacturing (ALM) is the industrial production name for 3D printing, a computer-controlled process that creates three dimensional objects by depositing materials, usually in layers.
Agile	In software development, agile (sometimes written Agile) practices include requirements discovery and solutions improvement through the collaborative effort of self-organising and cross-functional teams with their customer(s) / end user(s), adaptive planning, evolutionary development, early delivery, continual improvement, and flexible responses to changes in requirements, capacity, and understanding of the problems to be solve.
Analytics process automation (APA)	APA is a technology that allows anyone in an entity to easily share data, automate tedious and complex processes, and turn data into results.
Application programming interface (API)	API is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software.
Autonomous system (AS)	An AS in networking is a collection of one or more associated Internet Protocol (IP) prefixes with a clearly defined routing policy that governs how the AS exchanges routing information with other autonomous systems.
COBIT	A framework created by ISACA for IT management and IT governance. <https://www.isaca.org/resources/cobit>.
COSO Internal control – integrated framework	Helps entities design and implement internal control considering the many changes in business and operating environments. <https://www.coso.org/Pages/default.aspx>.
Intelligent automation (IA)	IA, or alternatively, intelligent process automation (IPA), is a software term that refers to a combination of AI and robotic process automation (RPA – q.v.).
Internal control	A process for assuring an entity's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations, and policies. A broad concept, internal control involves everything that controls risk to an entity.
Internal control environment	The overall attitude, awareness and actions of directors and management (ie 'those charged with governance') towards the internal control system and its importance to the entity. It is expressed in management style, corporate culture, values, philosophy and operating style, the entity structure, and human resources policies and procedures.
Internal control framework	A structured guide that systematically arranges and classifies expected controls or control topics.
IT general controls (ITGCs)	ITGCs are controls that apply to all systems, components, processes, and data for a given entity or information technology (IT) environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations.
Lo-Code / No-code	Lo-code/no-code development platforms are types of visual software development environments that allow enterprise developers and citizen developers to drag and drop application components, connect them together and create mobile or web applications.
Process modelling	Process modelling is the graphical representation of business processes or workflows. As in a flow chart, individual steps of the process are drawn out so there is an end-to-end overview of the tasks in the process within the context of the business environment.
Micro-services	A self-contained piece of business functionality with clear interfaces, that may, through its own internal components, implement a layered architecture. Micro-services may be implemented to address a short-term business need, often involving rapid developments using component applications.
Radio-frequency dentification (RFID)	RFID uses electromagnetic fields to automatically identify and track tags attached to objects.
Robotic process automation (RPA)	RPA is a form of business process automation that allows anyone to define a set of instructions for a robot or 'bot' to perform. RPA bots are capable of mimicking most human-computer interactions to carry out high-volume error-free tasks rapidly.
SOC 2® – SOC for Service Organizations: Trust Services Criteria	These reports are intended to meet the needs of a broad range of users who need detailed information and assurance about the controls at a service provider, relevant to security, availability, and processing integrity of the systems the service provider uses to process users' data and the confidentiality and privacy of the information processed by these systems. <https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report>.
The Three Lines Model	Helps entities identify structures and processes that most effectively assist the achievement of objectives and facilitate strong governance and risk management. <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf>.
Waterfall model	The waterfall model is a breakdown of project activities into linear sequential phases, where each phase depends on the deliverables of the previous one and corresponds to a specialisation of tasks. The Systems Development Lifecycle is an example of this.

Appendix – Survey demographics

The survey that formed part of the research activities for this report received 1,956 responses from ACCA, IMA and IIA members worldwide. An analysis of these responses is given in the following graphs.

General assumptions

- For the purpose of consistency, most of the analysis used globally aggregated data, which included input from the entire survey population.
- The survey was conducted online in March 2022.

Analysis of responses

Figure A1: Responses by region (n = 1,956)

- Western Europe, **24%**
- Africa, **21%**
- Asia-Pacific, **19%**
- North America, **12%**
- South Asia, **10%**
- Middle East, **6%**
- Caribbean, **4%**
- Central and Eastern Europe, **3%**
- Central and South America, **1%**

Figure A2: Responses by sector (n = 1,816)

- Corporate sector – small / medium sized, **20%**
- Corporate sector – large, **20%**
- Public sector, **13%**
- Financial services – small / medium sized, **9%**
- Financial services – large, **8%**
- Not-for-profit, **7%**
- Small or medium-sized practice (SMP), **7%**
- Other, **6%**
- Big Four accounting firm, **4%**
- Not currently working/ career break/ retired, **3%**
- Mid-tier accounting firm, **2%**
- Other international accounting firm, **1%**

Figure A3: Responses by entity size (n = 1,850)

- 0 – 9 employees, **8%**
- 10 – 49 employees, **14%**
- 50 – 249 employees, **21%**
- 250 – 999 employees, **20%**
- 1,000 +, **37%**

Figure A4: Responses by respondent (n = 1,956)

- Principally in business (such as working in a finance, accounting, or internal audit team or providing finance services across the organisation), **80%**
- Principally in public or other practice (such as an accountancy firm and undertaking audit, attestation, advisory and / or tax), **20%**

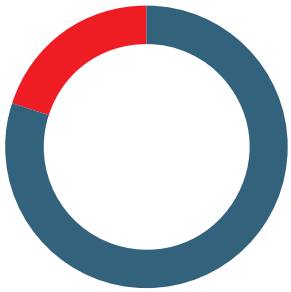


Figure A5: Responses by role (n = 1,854)

- Internal Auditor / Financial compliance, **13%**
- Financial Accountant, **11%**
- Finance / Operation Manager, **8%**
- Chief Financial Officer (CFO), **7%**
- Audit Manager, **7%**
- Financial Controller / Head of Compliance, **6%**
- Head of Finance / Director, **6%**
- Audit Senior Manager, **4%**
- Consultant, **4%**
- Management Accountant, **4%**
- External Auditor, **3%**
- Other, **27%**

Acknowledgements

The contributions of the following individuals in the development of this research are noted with thanks.

Khyam Abdulah, Pan-American Life Assurance Group, Trinidad and Tobago
Hashim Ahmed, Jaguar Mining Inc, Canada
Alper Alptekin, SOCAR Türkiye, Türkiye
Sandy Ardern, TD Asset Management, Canada
Victoria Armitage, GT, Republic of Ireland
Eban Bari, Triple Flag Precious Metals, Canada
Val Baynes, Commonwealth Bank, Australia
Robert Belle, Smip Consultancy, Kenya
Michael Bencsik, Cacel Pty Limited, New Zealand
Stan Bigford, Trenton Cold Storage Inc, Canada
Ruxandra Bilius, Baker Tilly Klitou & Partners SRL and IIA Romania, Romania
Harry Briggs, KPMG LLP, UK
Dermot Byrne, An Roinn Caiteachais Phoiblí agus Athchóirithe, Republic of Ireland
Ömer Çetin, KPMG, Türkiye
Lisa Coulman, Nobul Corporation, Canada
Niko Džepina, Asseco Central Europe, Slovakia
Carly Eaton, Provident Financial Group, UK
Andrew Elsby-Smith, Amtico, UK
Alex Falcon Heurta, Soaring Falcon, UK
Rashika Fernando, MDC Computers, Canada
Krystal George, TTPOST, Trinidad and Tobago
Anirban Ghosh, Wipro Ltd, India
Lee Glover, Haines Watson Controls & Assurance, UK
James Heather, Blackrock, UK
Hussein Hussein, Deloitte, Australia
Paul D. Hyman, Kingston Freeport Terminal, Jamacia
Mir Fahad Iqbal, Northern Trust Corporation, US
Ashish Jhaver, Barclays, India
Jodi Joseph, Adapt IT, South Africa
Javier Jurado, U S Bank, USA
Paul Kaczmar, Michael Page, UK
Stephen Kenny, Bank of Ireland, Republic of Ireland
Paula Kensington, PK Advisory, Australia
Rahul Kumar, EY, India
Jaishree Lam, Guyana Power and Light, Guyana
Leong, Singapore
Thea J Lowe, TJL Consulting Services, Barbados
Olga Lukashenko, Reanda Netherlands, Netherlands
Reshma Mahase, Davidson & Co LLP, Canada
Natalie Makoni, Servest, South Africa
Luka Matkovic, Czechia
Nauman Mian, bayt.net, UAE
Maja Milosavljevic, OMV, Austria
David Minas, Discount Car and Truck Rentals. Canada
Thapelo Modisagae, FNB Enablement Segment, South Africa
Julius Mojapelo, The Institute of Internal Auditors South Africa, South Africa
Brad Montierio, The Institute of Internal Auditors, USA
Kelvin Musana, Standard Chartered, Uganda
Av. Murali, Standard Chartered Bank, India
Ian Ng, AMMEGA, mainland China
Ebuka (Raphael) Nkemdilim, Wilfrid Laurier University, Canada
Joyce Nkini-Iwisi, Control Risks, Nigeria
Rolanke Oladapo, Control Risks, South Africa
Joseph Owolabi, Rubicola, Australia
Shreyash Pai, Livspace, India
Siobhan Pandya, Mary Kay Inc, USA
Michael Parkinson, Michael Parkinson Consultancy, Australia
Ann Patterson, St. Felix Centre, Canada
Atif Perez, Athabasca University, Canada
Juzar Pirbhai, Canadian Public Accountability Board, Canada
Mihaela Pop, WPP, Australia
Melanie Proffitt, Farncombe Estate, UK
Jürgen Pühler, BASF SE, Germany
Parthasarathy Ramaswamy, RGN Price & Co, India
Beate Randulf, National Bank of Greece, Greece
Rahul Ranjan, India
Simon Rose, Crest Nicholson, UK
Brendan Sheehan, White Squires, Australia
Heather Smith, ANISE Consulting, Australia
Mustafa Sönmez, ÜNLÜ & Co, Türkiye
Neville de Spretter, AdLibero2 Ltd, UK
Saravanan Srinivasan, Super Stahl Private Limited, India
Dirk Strydom, The Institute of Internal Auditors South Africa, South Africa
Sachin Tayal, Protiviti, India
Leslie Thompson, TRG, USA
Senol Toygar, TEB, Türkiye
Brian Tremblay, Onapsis Inc, USA
Engin Turan, Alternafi Bank, Türkiye
Robert van der Klauw, Munich Re, UAE

ACCA, IMA and The IAF would also like to thank all those who kindly completed the survey.

Authors

Clive Webb, Head of Business Management, ACCA
Laura LeBlanc, Director – Research & Insights, Institute of Internal Auditors
Loreal Jiles, Vice President, Research and Thought Leadership, Institute of Management Accountants

References

ACCA (2020), *The Digital Accountant: Digital Skills in a Transformed World*, <https://www.accaglobal.com/gb/en/professional-insights/technology/The_Digital_Accountant.html>, accessed 1 April 2022.

ACCA (2021), *Professional accountants at the heart of sustainable organisations*, <https://www.accaglobal.com/gb/en/professional-insights/pro-accountants-the-future/pro-accountants-heart-sustainable-orgs.html>, accessed 3 April 2022.

ACCA / CA ANZ (Chartered Accountants Australia and New Zealand) / Generation CFO (2021), *Transformational Journeys: Finance and the Agile Organisation*, <https://www.accaglobal.com/gb/en/professional-insights/technology/transformational-journeys.html>, accessed 1 April 2022.

ACCA / CA ANZ / KPMG (2018), *Embracing robotic automation during the evolution of finance*, <https://www.accaglobal.com/gb/en/professional-insights/technology/embracing-robotic-automation-during-the-evolution-of-finance.html>, accessed 3 April 2022.

ACCA / CA ANZ / Macquarie University (2019), *Cyber and the CFO*, <https://www.accaglobal.com/gb/en/professional-insights/technology/cyber-and-the-cfo.html>, accessed 3 May 2022.

ACCA / IMA / CIPS (Chartered Institute of Procurement and Supply) (2022), *Supply Chains – A Finance Professional's Perspective*, <https://www.accaglobal.com/gb/en/professional-insights/global-profession/supply-chains-post-pandemic-world.html>, accessed 3 April 2022.

ACCA / PwC (2021), *Finance Functions: Seizing the Opportunity*, <https://www.accaglobal.com/gb/en/professional-insights/pro-accountants-the-future/finance-functions-seize-opportunity.html>, accessed 1 April 2022.

Alspach, K, (2022), *Ransomware attacks surged 2X in 2021, SonicWall reports*, <https://venturebeat.com/2022/02/17/ransomware-attacks-surged-2x-in-2021-sonicwall-reports/>, accessed 3 May 2022.

Ashby, S., Bryce. C., and Ring, P. (2019), *Risk and performance: Embedding risk management*, <https://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/embedding-risk/pi-embedding-risk-management.pdf>, accessed 3 May 2022.

Burns, J., Steele, A., Cohen, E. E. and Ramamoorti, S. (2021), *Blockchain and Internal Control – the COSO Perspective*, <https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf>, accessed 19 April 2022.

Calagna, K., Cassidy, B., and Park, A. (2021), *Realize the Full Potential of Artificial Intelligence – Applying the COSO Framework and Principles to Help Implement and Scale Artificial Intelligence*, <https://www.coso.org/Documents/Realize-the-Full-Potential-of-Artificial-Intelligence.pdf>, accessed 19 April 2022.

COSO (2013), *Internal Control – Integrated Framework: Executive Summary*, <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf>, accessed 1 April 2022.

COSO (2017), *Enterprise Risk Management—Integrating with Strategy and Performance*, <https://www.coso.org/Pages/ERM-Framework-Purchase.aspx>, accessed 19 April 2022.

COSO (2022), *COSO-Board-Approves-Study-on-Sustainability-ESG*, <https://www.coso.org/news/Pages/COSO-Board-Approves-Study-on-Sustainability-ESG.aspx>, accessed 19 April 2022.

EFRAG (2022), *[Draft] European Sustainability Reporting Standard G1: Governance, risk management and internal control*, <https://www.efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FSiteAssets%2FFinal%2520Draft%2520ESRS%2520G1_22-03-14.pdf&AspxAutoDetectCookieSupport=1>, accessed 3 May 2022.

FRC (Financial Reporting Council) (2005), *Internal Control: Revised Guidance for Directors on the Combined Code*. Downloadable from <https://www.icaew.com/technical/corporate-governance/codes-and-reports/turnbull-report>, accessed 20 April 2022.

Grob, M. and Cheng, V. (2021), *Enterprise Risk Management for Cloud Computing*, <https://www.coso.org/Documents/COSO-ERM-for-Cloud-Computing.pdf>, accessed 19 April 2022.

Heier, J. R. Dugan, M. T. and Sayers, D. (2005), 'A Century of Debate for Internal Controls and their Assessment: a Study of Reactive Evolution', *Accounting History*, 10 (3) <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1023.3544&rep=rep1&type=pdf>, accessed 1 April 2022.

ICAEW (Institute of Chartered Accountants of England and Wales) (1999), *Internal Control: Guidance for Directors on the Combined Code*, <https://ecgi.global/download/file/fid/9442>, accessed 1 April 2022.

IIA (2020), *The IIA's Three Lines Model – An update of the Three Lines of Defense*, <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf>, accessed 1 April 2020.

IIA / Auditboard (2020), *Internal Audit's Digital Transformation Imperative: Advances Amid Crisis, Analyzing the Impact of 2020 on Internal Audit Functions' Implementation of Technology*, <https://web.theiia.org/cn/atxbg/Dig_Transform_Imperative>, accessed 8 April 2022.

ISSB (2022a), *[Draft] IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information*, <https://www.ifrs.org/content/dam/ifrs/project/general-sustainability-related-disclosures/exposure-draft-ifrs-s1-general-requirements-for-disclosure-of-sustainability-related-financial-information.pdf>, accessed 3 April 2022.

ISSB (2022b), *[Draft] IFRS S2 Climate-related Disclosures*, <https://www.ifrs.org/content/dam/ifrs/project/climate-related-disclosures/issb-exposure-draft-2022-2-climate-related-disclosures.pdf>, accessed 3 April 2022.

Jiles, L. (2020), *Transforming the Finance Function with RPA*, <https://www.imanet.org/-/media/8530486050e34be392772caa088f1162.ashx?la=en>, accessed 3 April 2022.

Jiles, L. (2021), *An Agile Approach to Finance Transformation*, <https://www.imanet.org/-/media/imanet-org/files/insights-and-trends/thought-leadership/the-future-role-of-management-accounting/agileandscrum_sma_report_final.ashx>, accessed 1 April 2022.

Kelly, M. (2022), 'Why IT General Controls are Important for Compliance and Cybersecurity' [website article], <https://hyperproof.io/resource/it-general-controls-compliance/>, accessed 19 April 2022.

Krumwiede, K. (2016), *Process Automation in Accounting and Finance*, <https://www.imanet.org/-/media/58e1aff5f8d74e4c92ac8f097db88321.ashx>, accessed 1 April 2022.

Krumwiede, K. (2017), *How to Keep your Job*, <https://www.imanet.org/insights-and-trends/the-future-of-management-accounting/how-to-keep-your-job?ssopc=1>, accessed 3 April 2022.

Lauren, D. (2017), *The History of Internal Control Systems*, <https://bizfluent.com/facts-7203983-history-internal-control-systems.html>, accessed 1 April 2022.

Maister, D. H., Galford, R., and Green, C. (2021), *The Trusted Advisor – 20th Anniversary Edition*, Free Press.

McPherson, A., and Sydney, C., *Comprehensive risk data: The new gold*, <https://www.pwc.com/gx/en/issues/risk-regulation/comprehensive-risk-data-the-new-gold.html?utm_campaign=5a1d7a5d94a3261aa2024207&utm_content=6262f8a941a0aa0001902d8e&utm_medium=smarpshare&utm_source=linkedin>, accessed 3 May 2022.

Schwab, K. (2015), *The Fourth Industrial Revolution: What It Means and How to Respond, Foreign Affairs*, <https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution>, accessed 3 April 2022.

SEC (Securities and Exchange Commission) (2022), *The Enhancement and Standardization of Climate-Related Disclosures for Investors*, <https://www.sec.gov/rules/proposed/2022/33-11042.pdf>, accessed 3 April 2022.

Sheen, A., (2020), *The Evolution of the Three Lines of Defence*, <https://www.acin.com/the-evolution-of-the-three-lines-of-defence/>, accessed 3 May 2022.

Statista (2021), *Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025*, Downloadable from <https://www.statista.com/statistics/871513/worldwide-data-created/>, accessed 1 April 2022.

Walker, P. L. (2022), *Enabling Organizational Agility in an Age of Speed and Disruption*, <https://www.coso.org/Documents/Enabling-Organizational-Agility-in-an-Age-of-Speed-and-Disruption.pdf>, accessed 18 April 2022.

Wright, C. (2021), *Future Ready: Upskilling Today for the Profession of Tomorrow*, <https://www.theiia.org/en/content/research/foundation/2021/future-ready-upskilling-today-for-the-profession-of-tomorrow/>, accessed 3 April 2022 (available to IIA members only).

PI-TRANSFORM-INTERNAL-CONTROL

ACCA The Adelphi 1/11 John Adam Street London WC2N 6AU United Kingdom / +44 (0)20 7059 5000 / **www.accaglobal.com**