Professional accountants – the future:

Ethics and trust in a digital age

HIGHLIGHTS

Think Ahead

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants, offering business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

ACCA supports its **198,000** members and **486,000** students in **180** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **101** offices and centres and more than **7,291** Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. It believes that accountants bring value to economies in all stages of development and seek to develop capacity in the profession and encourage the adoption of global standards. ACCA's core values are aligned to the needs of employers in all sectors and it ensures that through its range of qualifications, it prepares accountants for business. ACCA seeks to open up the profession to people of all backgrounds and remove artificial barriers, innovating its qualifications and delivery to meet the diverse needs of trainee professionals and their employers.

More information is here: www.accaglobal.com

Thank you to the following organisations for their support:

IFAC International Federation of Accountants®

CHARTERED ACCOUNTANTS™ AUSTRALIA + NEW ZEALAND

ICPAK

ima® The Association of Accountants and Financial Professionals in Business

Zambia Institute of Chartered Accountants (ZICA)

Special thanks to:

Ken Siong, technical director of the International Ethics Standards Board for Accountants (IESBA) for review and guidance

About the author:

Narayanan Vaidyanathan, head of technology insight, ACCA.

September 2017

Foreword

Ethical behaviour is normally associated with 'doing the right thing'. For professional accountants this involves much more than just an intuitive sense of following one's conscience. While that is certainly important, being ethical also brings with it specific expectations, such as demonstrating professional competency in the role being performed, exercising due care towards stakeholders and acting to uphold the public interest.

This report's approach to ethics is anchored in three facets that reflect ACCA's priorities in this area, as well as our mission and core values as a professional accountancy body.

Firstly, it is future-looking, with an emphasis on new or emerging ethical considerations in an evolving digital age.

Secondly, it takes an applied approach that assesses ethical implications with respect to specific digital themes and real-world situations.

Thirdly, it reflects a global point of view, with perspectives informed by over 10,000 survey respondents across 158 countries, and roundtable discussions with senior practitioners in nine countries.

The global accountancy profession has an important role to play in ensuring that organisations of all sizes adhere to the highest ethical and governance standards.

ACCA firmly believes in the value and importance of ethical behaviour – both as a necessary attribute of being a professional accountant and as a driver for sustainable organisational performance. We will continue to lead in this important thinking to ensure that ACCA and its members and students are best placed to drive ethical behaviour across the global economy.

Helen Brand OBE
Chief executive
ACCA

Executive summary

Ethical behaviour is a core attribute for professional accountants. Early in 2017, ACCA carried out global surveys of attitudes to ethics among over 10,000 professional accountants (including trainees), and among over 500 senior ('C-suite'[1]) managers.

More than 8 in 10 of these accountants around the world were of the view that strong ethical principles and behaviour will become even more important in the evolving digital age. This view was echoed by a similar proportion of C-suite executives, referring to the accountants in their organisations. Furthermore, 9 in 10 professional accountants agree that ethical behaviour helps to build trust in the digital age.

And almost all (95%) C-suite executives think that the accountant's ethical behaviour helps the organisation build trust with internal and external stakeholders. In other words, technology may have an impact on the details one needs to understand in order to be ethical, but it does not change the importance of being ethical.

The fundamental principles for accountants, established by the International Ethics Standards Board for Accountants (IESBA), still apply and remain relevant in the digital age, according to 94% of respondents.

When asked whether professional accountants act in the public interest, the majority agreed, with those who were employed more likely to agree (four out of five) than those who were not[2] (two-thirds).

Professional accountants most frequently cited upholding their own professional code as a way of contributing to the organisation's ability to uphold ethics, with more than three out of four respondents choosing this option – a view that 'ethics begins with me'. Embedding ethical standards in day-to-day procedures was the next most frequently cited, and was chosen by more than two-thirds of respondents. While this is important, embedding ethics into the strategy or business plans was picked by fewer respondents, with only about half of those employed seeing this as a way to contribute.

This may suggest a need to combine a procedural or tactical understanding with a wider view – something that might become particularly important when looking ahead to new or previously unseen situations in a digital context. If procedures have not been tested and well understood over several years, say if dealing with a new area such as internet-platform-based operations, then understanding the overarching strategy and purpose becomes particularly important. Otherwise, there may be a risk of compromising ethics through unintended consequences or performing the wrong procedure.

When commenting on the support needed to promote ethical behaviour in the organisation, strong leadership was cited as the top factor, chosen by about two-thirds of respondents. As mentioned earlier, senior professionals attach a high level of importance to ethics, so this might suggest a degree of alignment between those seeking support from leadership, and the willingness of leaders to provide it.

Fewer than half of respondents cited a well-publicised 'speak-up' policy, with appropriate anonymity or protection

1 Operating at CEO, or other board level leadership roles

2 Not currently working/career break/retired/full time student

> The professional accountant of the future[3] will need, in addition to technical capability, a rounded skill set that demonstrates key quotients for success in areas such as experience, intelligence, creativity, digital skills, emotional intelligence and vision. And at the heart of these lies the ethical quotient.

features. And only a little over half of respondents reported incidents or saw such reporting as a way of contributing to their organisation's efforts to uphold ethics. This leaves a substantial minority who did not report an incident, or did not see reporting of bad practice as a way of contributing, or who did not seek a well-publicised 'speak-up' policy in their organisations.

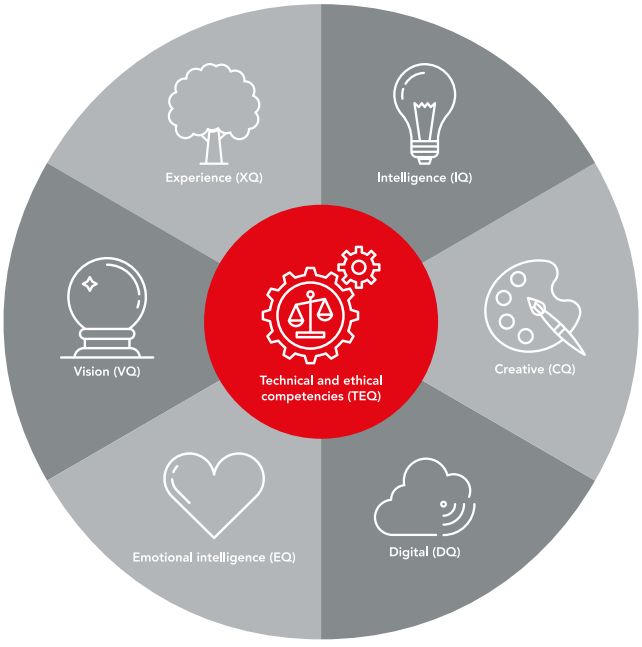
These findings may suggest the need to explore whether there is sufficient support and encouragement to ensure that professional accountants feel able to report unethical behaviour. Reporting of unethical behaviour may need further strengthening to be more effective in helping professional accountants to act as the 'ethical conscience' of their organisations. In addressing this, though, it will be important to understand the particular situation of the organisation. For instance, 'speak-up' behaviours may flow more naturally when the culture is more aware and supportive of ethical conduct; in other words forced imposition of a policy may not always be the most effective method of creating an ethical culture.

In order to lend specificity to the analysis of ethics in a digital environment, ethical aspects were identified across six digital themes. These themes were cybersecurity; platform-based business models; big data and analytics; cryptocurrencies and distributed ledgers; automation, artificial intelligence and machine learning; and procurement of technology. This highlights report examines Ransomware as an example.

The observations are informed by discussions with senior finance professionals, typically at the level of CFO, partner or equivalent. In the context of these digital themes, the IESBA fundamental principle which emerged most frequently as being at risk of compromise was professional competence and due care. This may be a reflection of the extent to which work situations in a digital age can present new information with ethical aspects that have not been seen before.

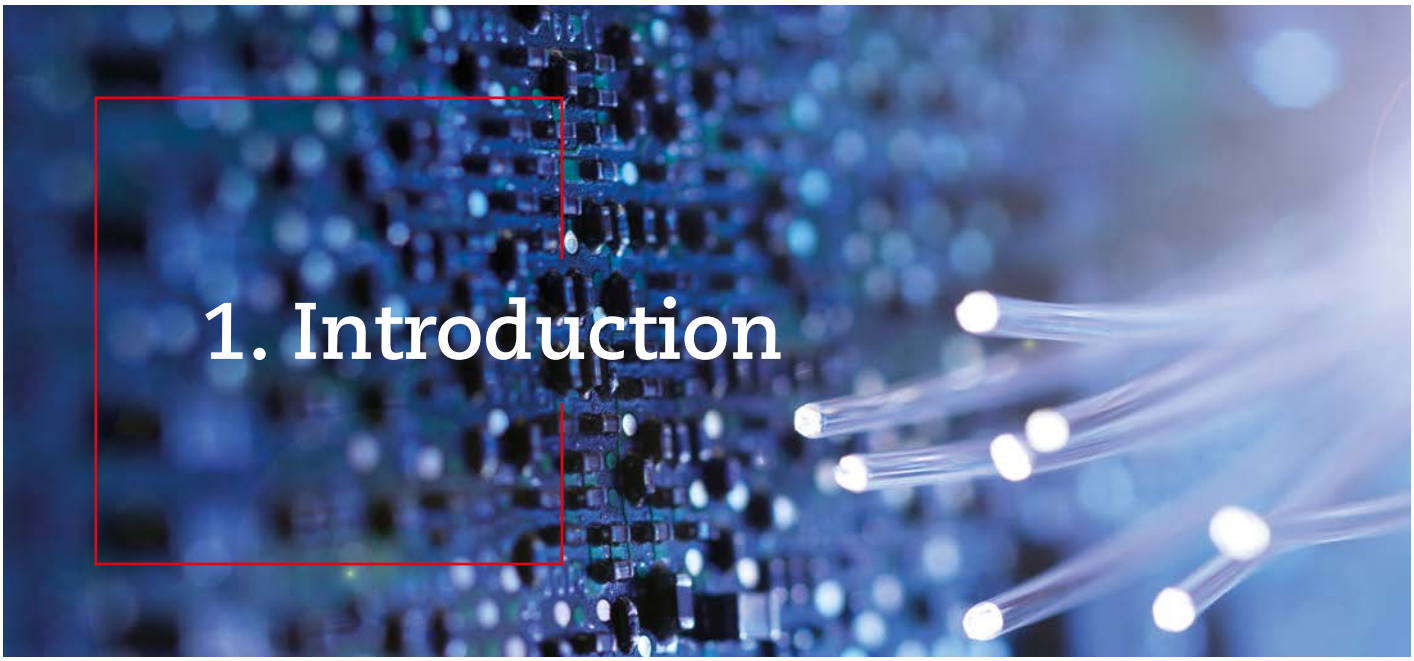
Looking ahead, it seems likely that risks of ethical compromises go way beyond issues of honest and straightforward professional and business relationships (integrity). For instance, it is difficult to apply ethical judgement to the use of distributed ledgers without a sufficient understanding of what they are. The professional accountant of the future will need, in addition to technical capability, a rounded skill set that demonstrates key quotients for success in areas such as experience, intelligence, creativity, digital skills, emotional intelligence and vision. And at the heart of these lies the ethical quotient.

Professional quotients for success



3 ACCA, *Professional Accountants – the Future: Drivers of Change and Future Skills*, 2016 <http://www.accaglobal.com/content/dam/members-beta/images/campaigns/pa-tf/pi-professional-accountants-the-future.pdf>, accessed 22 July 2017.

Contents



1. Introduction

1.1 REPORT STRUCTURE

The report addresses the aspects illustrated in Figure 1.1.

ACCA conducted an in-depth global survey in Q1 2017 to obtain the views of professional accountants, or those training to become such, on ethics and trust in a digital age. The survey was completed by respondents in 158 countries. Over 10,000 respondents completed the survey, of whom roughly 40% were ACCA members, 55% were ACCA students and the remaining 5% were members/students of other professional accountancy bodies.

In addition, to get a view of how accountants are perceived by others, 510 C-suite respondents who interact with the accountants in their organisations were also surveyed. Unless there is a specific mention of this group in a chart, it may be assumed that responses refer to the 10,000+ respondents.

The approach is to explore ethical questions that may arise in each of six digital themes, and to consider response options available to the professional accountants. The observations are informed by discussions with senior finance professionals, typically at the level of CFO, partner or equivalent. These perspectives were gathered via roundtable discussions conducted in Australia, China, Kenya, Nigeria, Republic of Ireland, Russia, Singapore, UAE and the US. In addition, the perspectives are informed by the experience and expertise of ACCA's Global Forums members.

The six digital themes examined are:

1. cybersecurity
2. platform-based business models
3. big data and analytics
4. cryptocurrencies and distributed ledgers
5. automation, artificial intelligence and machine learning and
6. procurement of technology.

To provide a sense of the issues involved, this summarised highlights report includes one ethical challenge for the theme of cybersecurity. For more detail, the main report explores two ethical challenges for each theme.

Figure 1.1: Key considerations pertinent to ethics and trust in a digital age

*Professional accountants

2. Values

2.1 IMPORTANCE OF ETHICS

When looking ahead, the vast majority of respondents are of the view that strong ethical principles and behaviour will become more important in the evolving digital age (Figure 2.1). This may be driven by the potential for a range of threats and associated breaches. This combined with the pace of change and the need to absorb new information specific to digital scenarios, may be driving the view that this area will become even more important in the future.

The vast majority of respondents supported the view that ethical behaviour does help to build trust in the digital age (Figure 2.2). This is important because the ability of professional accountants to create value depends crucially on their ability to win the trust of their stakeholders. In a fast-evolving digital age, clients and other stakeholders are much more likely to continue investing their trust in the accountant if they believe that this individual will always act in an ethical manner.

Figure 2.1: Strong ethical principles and behaviour will become more important in the evolving digital age

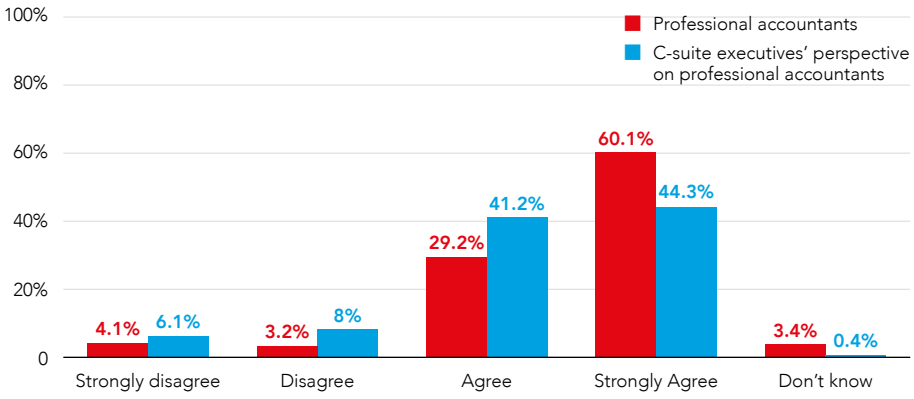
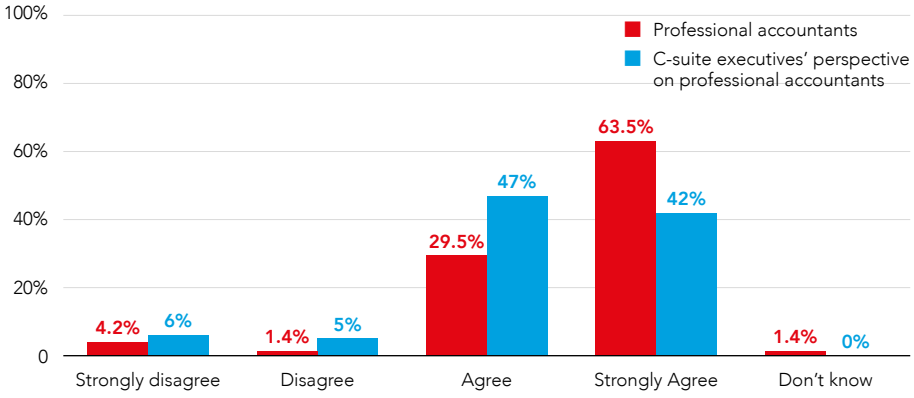


Figure 2.2: Extent to which respondents agree that ethics helps to build trust



> Almost all C-suite respondents agreed that the accountant's ethical behaviour helps the organisation to build trust with internal and external stakeholders.

In addition, C-suite executives were asked a more specific question about the link between the ethics of the accountant and the ability of the organisation to build trust with internal and external stakeholders (Figure 2.3). Almost all C-suite respondents agreed that the accountant's ethical behaviour helps the organisation to build trust with internal and external stakeholders, with 42% being of the view that it helps to a very significant degree.

2.2 RELEVANCE OF IESBA PRINCIPLES

Given the importance of ethics, the associated question is whether the IESBA's ethical principles for professional accountants remain relevant. Survey respondents were overwhelmingly of the view that they certainly do remain relevant (Figure 2.4). This may be linked to the fact that, being principles rather than prescriptive rules, they place a responsibility on the professional accountant to apply them to a given situation rather than blindly following a check-box compliance approach.

Figure 2.3: A view from the top: C-suite executives think that the accountant's ethical behaviour helps the organisation build trust with internal and external stakeholders

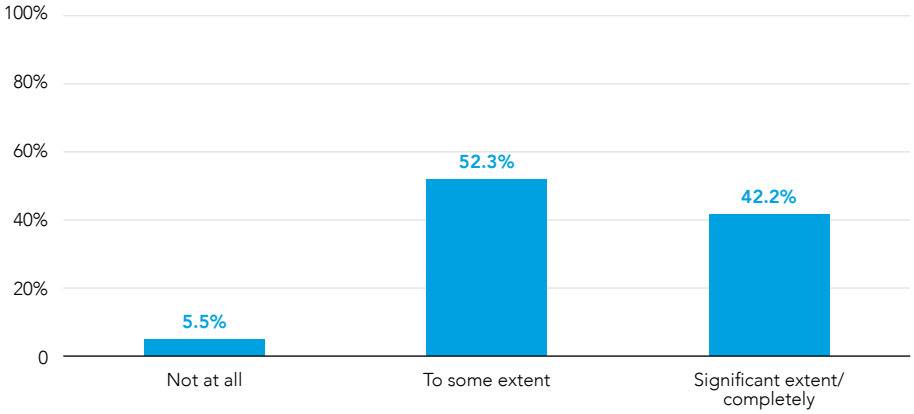
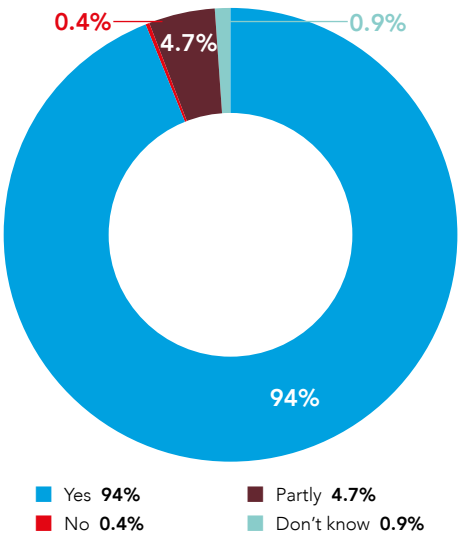


Figure 2.4: IESBA principles still apply and remain relevant



3. Experiences

3.1 ETHICAL CHALLENGES FACED

About one in five respondents reported that they had personally experienced pressure to compromise their ethical principles in the preceding 12-month period (Figure 3.1).

Of particular concern, however, is that a little under half of these respondents did not report the incident in which they had experienced pressure to compromise (Figure 3.2). This may be reflective of various underlying reasons, such as a wider culture of acceptance of the unethical behaviour concerned, or the lack of a well-communicated organisational ethics policy.

The survey also asked about situations where the respondent observed behaviour that could compromise ethics, either in their own organisation or at a client (Figure 3.3).

Looking across personally experienced instances as well as those that had been observed, it is apparent that challenges do appear from time to time – with 2 to 3 in every 10 respondents having been exposed (directly or indirectly) to an ethical problem in the last 12 months.

Those that had been exposed to an ethical challenge were further asked which ethical principles (as defined by the IESBA) they thought had been compromised. The responses revealed that the most commonly compromised principle was that of integrity – in other words, being straightforward and honest in all professional and business relationships (Figure 3.4).

Figure 3.1: Respondents who had experienced pressure to compromise their ethical principles in the previous 12 months

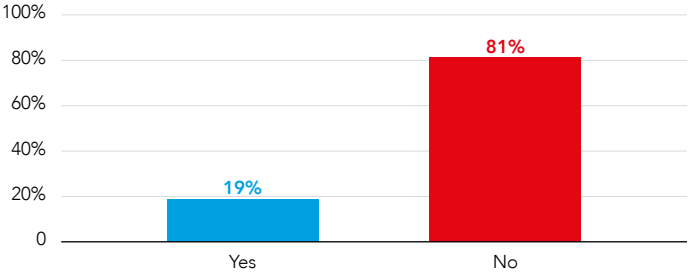


Figure 3.2: Respondents who reported the incident in which they had experienced pressure to compromise their ethical principles

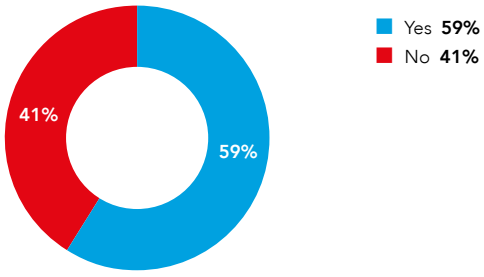


Figure 3.3: Respondents who observed behaviour in the last 12 months that compromised ethics at their own organisation or at a client organisation

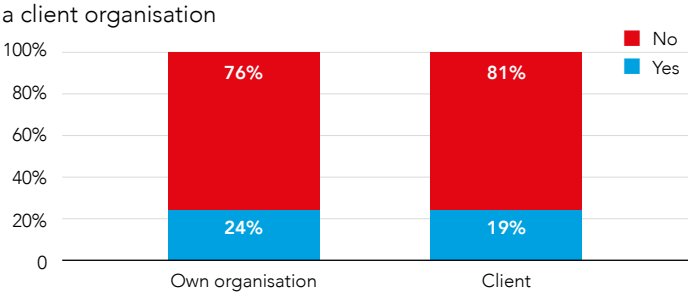
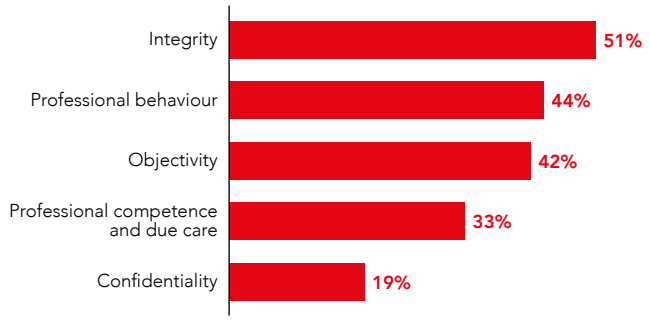


Figure 3.4: Ethical principles that were compromised in a situation that was personally experienced or observed



4. Application of an 'ethical lens' to digital themes

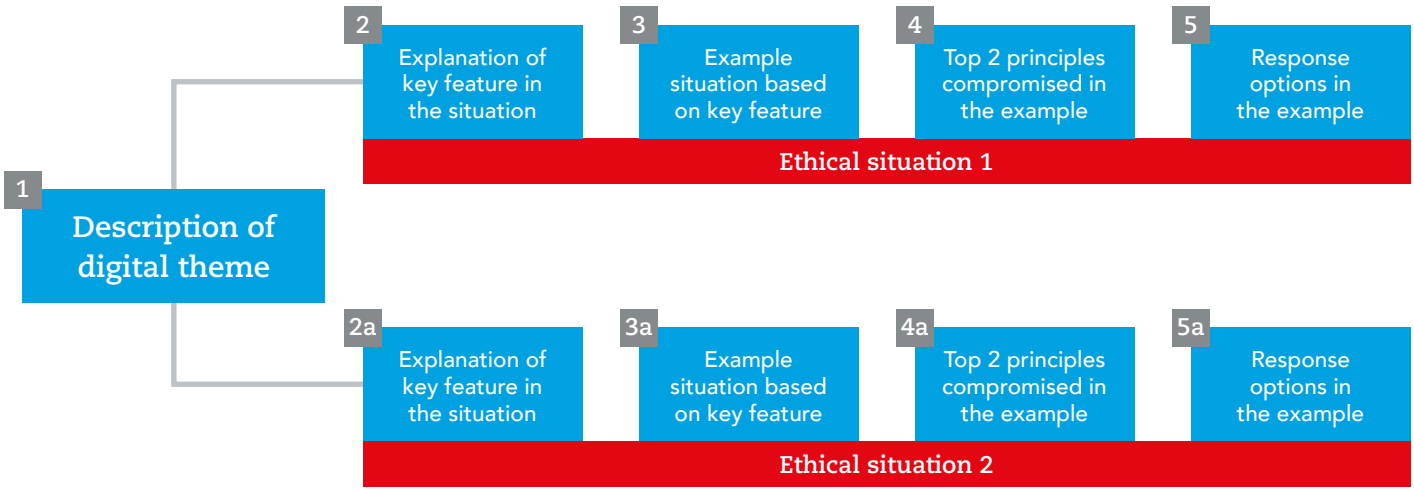
In order to lend specificity to the analysis of ethics in a digital context, six digital themes have been chosen. For each theme two ethically challenging situations have been identified and assessed against the IESBA principles.

The aim is to identify the top two IESBA principles that could be compromised within each ethically challenging situation and then to reflect briefly on response options for that situation (Figure 4.1).

This assessment is done both from the perspective of the accountant in business and the auditor (depending on the situation, reference may be to internal auditors, external auditors, or both).

This view is informed by discussions with senior finance professionals, typically at the level of CFO, partner or equivalent. The perspectives were gathered from roundtable discussions conducted in Australia, China, Kenya, Nigeria, Republic of Ireland, Russia, Singapore, UAE and the US. In addition, the perspectives are informed by the experience and expertise of ACCA's Global Forum members.

Figure 4.1: Layout of information: applying an ethical lens to a digital theme



Looking ahead, it seems likely that risks of compromise go way beyond issues of honest and straightforward professional and business relationships.

The choice of the top two principles that have been compromised is informed by discussions with senior finance professionals, typically at CFO, partner level or equivalent. They were asked to consider the likelihood and frequency of compromise, as well as the seriousness of the impact from such a compromise (Figure 4.2).

The six digital themes examined in the full report are:

1. cybersecurity
2. platform-based business models
3. big data and analytics
4. cryptocurrencies and distributed ledgers
5. automation, artificial intelligence and machine learning, and
6. procurement of technology.

This highlights report examines Ransomware as an example.

As shown in Figure 4.2, the principle that was most frequently cited as being under threat of compromise was professional competence and due care. This may be a reflection of the extent to which ethically challenging situations in a digital age can present new problems that have not been seen before.

Reacting properly requires building up a high standard of knowledge and understanding of the situation and its context before being able to act in an ethical manner. A lack of knowledge and expertise will create the risk of compromising professional competence and due care obligations.

When accountants reflected on principles that were compromised in the recent past (Figure 3.4), integrity featured very highly. Looking ahead, it seems likely that risks of compromise go way beyond issues of honest and straightforward professional and business relationships. It is difficult to apply ethical judgement on the use of distributed ledgers for example, without an understanding of what they are, and the opportunities and challenges they pose.

Figure 4.2: IESBA principles at risk of compromise for accountants in business and auditors across all six digital themes

4.1 DIGITAL THEME: Cybersecurity

Cybersecurity encompasses wide-ranging threats to computers, networks, data and programs. Viruses, malware and other forms of cyberattack can cause havoc through system outage, data theft or denial of service – any of which has serious reputational and financial impact.

Data theft

Data theft is the most immediate and common impact of a breach in cybersecurity. Organisations hold a lot of valuable data in a variety of systems. Some organisations may use proprietary software, while others may rely more on open-source code. Some software might be fully owned and paid for by the organisation while others might be licensed via monthly subscription, for example where the provision is through a cloud service. The data itself could be internal (eg employee-related) or external (eg customer-related). Whatever the scenario, the effects of data theft include financial loss and reputation/brand damage.

4.1.1 EXAMPLE SITUATION: Ransomware

Hackers expose the vulnerability in an open-source database where commercial implementations have not been adequately secured. The organisation is compromised, with all the data in the system having been deleted and a note left by the hacker. The hacker claims to have retained a copy of the data and will return it on payment of a 0.5 bitcoin[4] payment to a specified account. There is no back-up of the data.

Compromise of ethical principles

ACCOUNTANT IN BUSINESS:	
Objectivity	There is a need to 'do the right thing', which may be to refuse to pay. While £1,000 may be within tolerance limits, but there is no guarantee that the data will be returned, or that more money will not be demanded. The risk that objectivity may be compromised arises from undue influence (intimidation from threats that data will be misused/destroyed), being allowed to override professional or business judgement.
Confidentiality	Ransom demands work best when there is a real cost (financial or reputational) should the data be out of the organisation's control – which is most likely to arise with confidential data. Whether or not customer data is covered by contractual confidentiality clauses, exposing it to unauthorised parties may breach the fundamental ethical duty of confidentiality.
AUDITOR:	
Professional competence and due care	For internal auditors, the risk can stem from having inadequate as well as infrequent review mechanisms. Cyberattacks are continually getting more sophisticated so lack of awareness of emerging developments could lead to ethical compromise.
Integrity	Internal auditors will need to be honest in their assessment of the procedures put in place to guard against cyberattacks, which are now a permanent issue. If it later emerges, for instance, that the internal auditor was aware that the latest security patches had not been used to secure the systems, questions might arise as to why this lapse had occurred.

Response to this situation

ACCOUNTANT IN BUSINESS:	
Preventing	IT security is at one level a technology issue but the accountant in a business (as a custodian of sensitive data) needs to be aware of the risks, and have knowledge of the techniques adopted by their organisation and others to address these.
Resolving	Whether or not the ransom is eventually paid, it is important that communications about the data loss are clear, controlled and transparent. The impression that facts are being suppressed is damaging. In many cases, it may be necessary to make affected customers aware as soon as possible that their data has been compromised. The accountant may need to advise management on these issues.
AUDITOR:	
Acting in the shareholder and public interest	External auditors may need to decide whether a public disclosure about the data loss is required. Public disclosure is a major decision and careful consideration will need to be given to whether this is appropriate and permissible.[5] Internal auditors may need to check whether the organisation has appropriate review mechanisms to allow incorporation of new/emerging cyber threats into existing risk-assessment processes.
Maintaining independence	If there is uncertainty on the best approach for dealing with the ransom demand, the external auditor might recommend seeking external guidance. This opinion may be based on the auditor's awareness of experts in this specialist area, but the auditor should remain independent and not have any involvement in the selection decision.

4 About £1,000 in June 2017.

5 Under the IESBA Code, public disclosure would only be permissible if (1) it is authorised by the client or organisation and not prohibited by law; (2) it is required by law; or (3) there has been an act of NOCLAR (non-compliance with laws and regulations), such act has caused actual or potential substantial harm to the public, and such disclosure would not be prohibited by law.

The asset base that we're trying to protect is changing, but also [those] whom we're protecting it from [have] changed as well. Traditionally, that protection would have been more internally focused, because clients would have people who had control of the assets, whereas today the risk is more likely to arise from external sources than internal – this is harder to foresee and protect against.

Derek Henry, Partner – Head of R&D, BDO

For organisations with an internal audit function, the role of internal auditors is always to ask the difficult questions. For cybersecurity, there is a long list of difficult questions to ask. These questions play a role in improving the level of [systems] maturity and making sure that organisations take cybersecurity seriously and have the right safeguards in place. There's also recent guidance from the Central Bank of Ireland that cybersecurity should be a standing item on Board agendas.

Gary McPartland, Associate Director, Grant Thornton

For us as accountants it is important that we understand where the threats are coming from or else we will be fooled by internal and external threats, such as ransomware; appropriate network security is needed to be in place at all times.

Kola Agunbiade, Chief Financial Officer, IS Internet Solutions (A division of Dimension Data)

If there is an unfortunate data leakage and the leakage could harm individuals or companies, an organisation should be transparent and inform all of those affected. Alerting customers and external parties that data has leaked, to enable them to contain information and change passwords, is fair and ethical. Organisations have a duty of care to let all people know who are affected by the leak.

Amanda Powell, Chief Financial Officer, ME Digital Group FZ LLC

Professional accountants have an obligation to act in the public interest. If there was a data breach, they should endeavour to inform the end user, the customer or the client, at the earliest opportunity and let them know that their confidential information has been exposed… [rather than] seeking to protect the interests or reputation of the organisation.

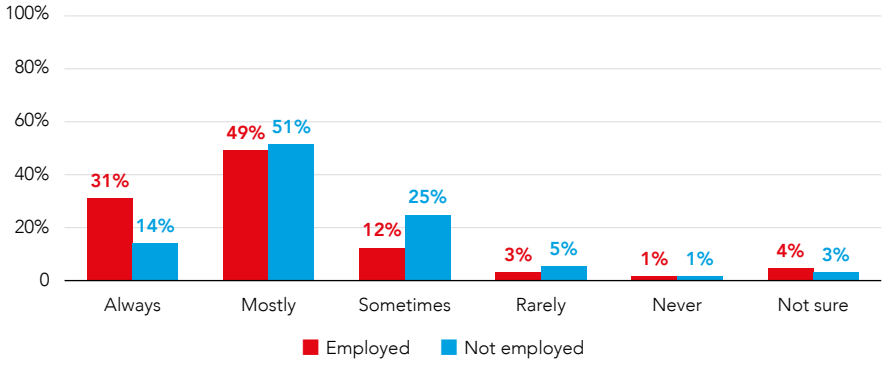
Ken Siong, Technical Director, IESBA

5. Responsibilities

5.1 ACTING IN THE PUBLIC INTEREST

This is a fundamental responsibility that goes to the heart of being a professional accountant. Four out of five employed respondents, and about two-thirds of those not employed[6], took the view that professional accountants act in the public interest 'Always' or 'Mostly' (Figure 5.1).

Figure 5.1: Do accountants themselves believe they act in the public interest?



5.2 UPHOLDING ETHICS IN THE ORGANISATION

5.2.1 Ethics begins with me

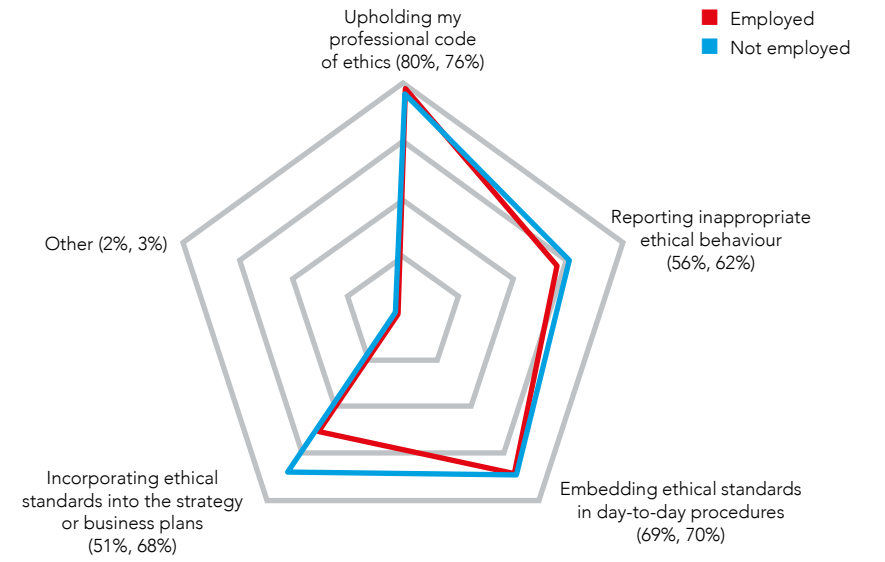
Respondents, whether they were employed or not, rated upholding their own professional code as the most frequently cited way of contributing to their organisation's ability to uphold ethics – with more than three-quarters of respondents choosing this option.

5.2.2 Connecting tactical and strategic

Embedding ethical standards in day-to-day procedures is cited the next most frequently – chosen by more than two out of three respondents. While this is important from a tactical point of view, embedding ethics into the strategy or business plans was picked by fewer respondents – only about half of those in employment.

This may suggest a need to combine a procedural or tactical understanding with a wider view – something that might become particularly important when looking ahead to new or previously unseen situations in a digital context. If procedures have not been tested and well understood over several years, say if dealing with a new area such as the adoption of internet-platform-based operations, then it becomes particularly important to understand the organisation's underlying strategy and purpose to avoid compromising ethics through unintended consequences or wrong procedures.

Figure 5.2: Professional accountants contributing to the organisation's ability to uphold ethics in a digital age



6 Not employed: not currently working/career break/retired/full time student

6. Support for promoting ethics in organisations

6.1 LEADERSHIP

Strong leadership to set the tone at the top was cited as the top area (by about two-thirds of respondents) where support is needed for promoting ethical behaviour in organisations.

6.2 ORGANISATIONAL CODE

The second most commonly cited need, chosen by just over half the respondents, was for support in creating, implementing and managing a code of ethics for the organisation ('ethics' here includes organisational values).

6.3 'SPEAK-UP' POLICY

Fewer than half the respondents said they would value the support of a well-publicised 'speak-up' policy, with appropriate anonymity or protection features. This facility is outside the top five areas for support cited by professional accountants. Only a little over half of respondents either reported incidents (Figure 3.2) or saw such reporting as a way of contributing to their organisation's upholding of ethics (Figure 5.2).

This leaves a substantial minority who did not report an incident, did not see reporting of bad practice as a way of contributing or do not want support with speak-up arrangements.

These findings may suggest the need to explore whether there is sufficient support and encouragement to ensure that professional accountants feel able to report inappropriate or unethical behaviour. Reporting of unethical behaviour may be an area that needs further strengthening in order to help professional accountants to act as the 'ethical conscience' of their organisations. In addressing this, however, it will be important to understand the particular situation of the organisation. For instance, 'speak-up' behaviours may flow more naturally when the culture is more aware and supportive of ethical conduct; in other words, forcing a policy may not always be the most effective approach.

Figure 6.1: Areas where support is needed for promoting ethical behaviour in organisations

7. Conclusion

To behave ethically and instil trust in a digital age, professional accountants will need to learn new information relatively quickly, and to apply their judgement to this information, often in situations they may not have seen before. The five IESBA fundamental principles provide a foundation, on the basis of which accountants can assess whether they are meeting the standards of ethical behaviour expected from them.

Looking ahead, it will be important to have an open mind that recognises the value of what has been learnt so far, but with an understanding that this has to be continually placed into the context of situations as they evolve.

At the very least it would seem beneficial for professional accountants to bear in mind the following as they navigate ethical situations in the digital age.

- **Build knowledge of emerging technologies and digital issues:** to reduce risk of compromise to professional competence and due care.
- **Combine process control with a strategic view:** to reduce the risk of unintended consequences.
- **Evaluate mechanisms for reporting unethical behaviour:** to reduce the risk of breaches.

PI-HIGHLIGHTS-ETHICS-TRUST-DIGITAL-AGE

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