

Agenda Item 5-D.4 (Reference Material)

IESBA and IAASB Joint Stakeholder Survey – A.3 Digital Transformation – Financial Crimes Enabled by Technology

05.01. 3 – Slightly decreasing in importance

12. Others

Eri Murakami (Wood Design Studio Inc.)

IESBA impacts large effects

3 – Slightly decreasing in importance

05.02. 4 – Slightly increasing in importance

05. Regulators and Oversight Authorities

Martina Morrissey (IAASA)

4 – Slightly increasing in importance

06. Jurisdictional and National Standards Setters (JSS)

Compagnie Nationale des Commissaires aux Comptes (CNCC) - Conseil National de l'Ordre des Experts Comptables (CNOEC)

4 – Slightly increasing in importance

Financial crime enabled by technology will certainly increase proportionately with technological evolution. The risk will probably be more of an issue in relation to compliance with various laws and regulations (anti-money laundering, fight against organized crime, terrorism, etc.) than an audit issue; at this stage, we have not identified a need to develop additional standards; NOCLAR, ISA 315 (Assessment of Cyber Risks), and ISA 240 (Fraud) already address regulatory requirements.

Japanese Institute of Certified Public Accountants (JICPA)

4 – Slightly increasing in importance

Royal Netherlands Institute of Chartered Accountants (NBA)

4 – Slightly increasing in importance

While evolving risks such as cyber threats may increase expectations on auditors, particularly in areas such as risk assessment and going concern, this does not in itself lead to a need for adjusted standards. The existing standards are sufficient to use in this context.

This trend can also relate to more collaboration with specialists and the increasing importance of the professional skepticism and judgement of the accountant. Any response, if needed, should focus on non-authoritative guidance or knowledge-sharing rather than the creation of new standards.

Wirtschaftsprüferkammer (WPK)

4 – Slightly increasing in importance

07. Accounting Firms

Forvis Mazars Global Limited (Mazars)

Financial crime, including Anti-Money Laundering, is primarily a jurisdictional legal and regulatory issue with significant variation in local requirements, and is therefore not an area where international standards would be appropriate. However, the Boards may consider non-authoritative guidance which could support application of existing standards (e.g. ISA 240 – Fraud; NOCLAR provisions) when considering financial crime that may occur at a client when performing an audit or assurance engagement.

4 – Slightly increasing in importance

Gats-Ratings Professionals

Technology for Crime should crease at higher pace

4 – Slightly increasing in importance

Piotr Witek (Moore Polska)

4 – Slightly increasing in importance

PricewaterhouseCoopers International Limited (PWC)

4 – Slightly increasing in importance

Our approach to assessing importance

In a rapidly evolving, technology-driven environment, technology-enabled financial crime may be expected to increase. However, we have assessed this trend as only slightly increasing in importance for the SSBs, reflecting our view that existing standards—including those addressing risk assessment and non-compliance with laws and regulations (NOCLAR)—already provide a robust foundation for practitioners. This assessment also reflects the need for proportionality: while incidence may rise, any SSB response is more likely to focus on targeted clarification of existing requirements rather than on redefining underlying principles or new standard setting activity. Nevertheless, as described in our response to trend A.1, the SSBs may need to give further specific consideration to how technology, and specifically AI, may be used to facilitate and/or conceal fraud.

Overarching comments

Both SSBs have addressed NOCLAR in relatively recent standard setting activities. Accordingly, the focus should be on assessing whether incremental guidance is warranted, particularly in relation to how technology enabled financial crime may affect practitioners' audit and ethical responsibilities.

Matters specific to the IAASB

In addition to evaluating whether non-authoritative guidance may be warranted in respect of ISA 250 (Revised), auditors may benefit from non-authoritative guidance addressing relevant considerations when obtaining an understanding of the entity, its environment and its system of internal control, relating to how an entity's use of technology may create opportunities for financial crime and pose a related risk of material misstatement of the financial statements (ISA 315 (Revised 2019)), and in applying ISA 240 (Revised). Such guidance could usefully also emphasise the scope of the auditor's responsibilities as it relates to financial crime committed by, or perpetrated against, the entity in the context of an audit of financial statements.

Matters specific to the IESBA

We encourage the IESBA to consider, as part of its post-implementation review, whether the current NOCLAR framework provides sufficiently clear guidance for professional accountants who encounter or suspect financial crime enabled by sophisticated technology. The use of digital assets and other technology-

enabled structures can obscure the identity of ultimate beneficiaries, creating practical compliance challenges for professional accountants in identifying and responding to potential non-compliance.

RSM International Limited

Increased risk driven by technology

Emerging technology can enable new forms of financial crime through increased automation, data volume and complexity. This is an important trend given the potential implications for fraud risk, misuse of technology and public trust in financial reporting. However, there is a risk that placing too much emphasis on technology-enabled financial crimes could unintentionally create an expectation that auditors are responsible for detecting all forms of technology-driven misconduct.

Fraud risk and auditing technology

It is important to maintain a clear distinction between the auditor's responsibilities in relation to fraud and those relating to technology. Auditors are not generally responsible for auditing the technology itself, but rather for auditing the outputs and financial information generated using the technology. While technology may facilitate financial crime, framing this as a separate workstream risks blurring expectations around the auditor's responsibilities, including when specialised forensic or technological expertise may be more appropriate.

Recent revisions to the fraud standard

IAASB issued 'International Standard on Auditing 240 (Revised), The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements', (the revised fraud standard) in July 2025, which is effective for audits of financial statements for periods beginning on or after 15 December 2026. We expect the revised fraud standard to address many of the underlying risks associated with fraud, including those enabled by technology, as described above. As such, we consider the importance of this trend will increase during the period 2028–2031 as firms implement International Standard on Auditing (ISA) 240 (Revised). However, we believe that elevating technology-enabled financial crimes as a significant priority before assessing how ISA 240 (Revised) is implemented and operates in practice may be premature for the 2028–2031 work plan. We support ongoing monitoring of the implementation of the revised fraud standard with a focus on identifying any issues or gaps that may require immediate action or clarification.

Evaluation of how auditors are evaluating and, when relevant, identifying technology-related financial fraud may be an important element of the post-implementation review of ISA 240 (Revised).

4 – Slightly increasing in importance

09. Public Sector Organizations

Sanford Rich (NYC Board of Education Retirement System)

4 – Slightly increasing in importance

I believe that transparency about financial crimes will be important to maintaining a regular cadence of responding to these risks. Unfortunately, I believe financial criminals will always be a step ahead with technology and the industry must be prompt with responses.

10. Member Bodies or Other Professional Accountancy Organizations

Institute of Singapore Chartered Accountants (ISCA)

While technology enabled financial crimes and cybersecurity threats continue to present risks, we expect their relative importance to increase slightly compared with other key trends identified in this survey.

4 – Slightly increasing in importance

Malaysian Institute of Accountants (MIA Malaysia)

4 – Slightly increasing in importance

Our approach to assessing importance

In a rapidly evolving, technologically driven landscape, an increase in technology-enabled financial crime is foreseeable. Nevertheless, we have assessed this trend as only slightly increasing in importance for the SSBs, reflecting our view that the existing standards — including those addressing risk assessment and non-compliance with laws and regulations (NOCLAR) — already offer a robust foundation for practitioners. This assessment also reflects the importance of proportionality: while the incidence of such crimes may rise, any SSB response is more likely to involve targeted clarification of existing requirements rather than a fundamental re-engineering of underlying principles or the initiation of new standard-setting activities. Nonetheless, as set out in our response to trend A.1, the SSBs may need to dedicate further specific consideration to the potential for technology, particularly AI, to facilitate or conceal fraudulent activities.

Overarching comments

Both SSBs have addressed NOCLAR through relatively recent standard-setting initiatives. Consequently, the forward-looking emphasis should be placed on evaluating whether incremental guidance is necessary, particularly concerning how technology enabled financial crime might impact practitioners' audit and ethical obligations.

In addition, continued engagement and coordination with regulators, law enforcement agencies and international organisations may help support more consistent approaches to addressing technology-enabled financial crime and strengthen confidence in the global financial reporting ecosystem.

Matters specific to the IAASB

Alongside evaluating whether non-authoritative guidance in respect of ISA 250 (Revised) is warranted; auditors may also find it helpful to have additional non-authoritative guidance. Such guidance would focus on relevant considerations when gaining an understanding of the entity, its environment, and its system of internal control. Specifically, it should address how an entity's utilization of technology might create opportunities for financial crime and introduce associated risks of material misstatement in the financial statements (ISA 315 (Revised 2019)), and how this should be applied within ISA 240 (Revised). This guidance could also usefully delineate the scope of the auditor's responsibilities pertaining to financial crime perpetrated by, or against, the entity in the context of a financial statement audit.

Matters specific to the IESBA

We recommend that the IESBA, as part of its post-implementation review, evaluates whether the current NOCLAR framework offers sufficiently clear guidance for professional accountants encountering or suspecting financial crime enabled by sophisticated technology. The inherent nature of digital assets and other technology-enabled arrangements can obscure the identification of ultimate beneficiaries, thereby presenting practical challenges for professional accountants in detecting and addressing instances of potential non-compliance.

The IESBA may also wish to consider whether further guidance is necessary to support professional accountants in balancing confidentiality obligations, professional judgment and public interest considerations when responding to increasingly complex technology-enabled financial crime scenarios.

Malta Institute of Accountants (MIA Malta)

4 – Slightly increasing in importance

Auditors could benefit from additional non-authoritative guidance on how technology use in an entity may lead to financial crime and affect risks in financial statement audits. Such guidance should clarify auditors' responsibilities regarding financial crime both committed by and against the entity.

05.03. 5 – Increasing in importance

02. Users of Financial or Non-Financial Information

Goro Kumagai (The Securities Analysts Association of Japan)

5 – Increasing in importance

International Corporate Governance Network (ICGN)

5 – Increasing in importance

As above, technology-enabled financial crime and cybersecurity risks may affect audit quality, assurance engagements and ethical responsibilities. The SSBs should consider whether existing standards and guidance remain adequate in areas such as professional scepticism, risk assessment, use of technology-enabled tools and responsibilities relating to non-compliance, fraud and financial crime.

Investment Company Institute

5 – Increasing in importance

Educating stakeholders
Implementation support
Engagement with technology and cybersecurity professionals

Kei Tsuchiya (The Securities Analysts Association of Japan)

I am concerned that advances in technology are making the execution and concealment of fraudulent activities relating to accounting treatments and disclosures increasingly sophisticated, exploiting digital systems, networks, and AI-enabled tools, and that such misconduct may not be adequately detected under existing audit and assurance standards.

5 – Increasing in importance

Martin Lawrence (Ownership Matters Pty Ltd)

5 – Increasing in importance

Cybercrime impacts on the financial statements and protections against cybercrime will become increasingly relevant

Takeshi Kimura (Nippon Life Insurance Company (Board Member, PRI) (Steering Committee Member, TISFD))

5 – Increasing in importance

Technology-enabled financial crimes and cybersecurity risks directly affect market trust. As capital markets become more digitized, the resilience of control environments and the ability of auditors to respond to technologically sophisticated misconduct will become increasingly important for maintaining systemic confidence.

03. Preparers or Issuers of Financial Statements or Other Information

Business Europe

5 – Increasing in importance

Technology-enabled financial crime creates new risks through speed, scale and distance, and may weaken traditional forms of external validation or supposed third-party verification. This has direct implications for audit evidence, fraud risk assessment, and the need to understand the business model, systems and control environment more deeply.

Cybersecurity risks—both within the audit firm and at the client—will also remain highly relevant. Over time, developments such as quantum computing may also affect encryption, authentication and the reliability of certain forms of digital evidence.

Responding to this would require close stakeholder engagement and rapid communication by the SSB's to the market, indicating that other methods than standard setting may be required – again building on the principles-based nature of the standards. This in turn requires less mandatory process-requirements and more focus on professional scepticism and competence to remain relevant and cost-effective

Sevdalina Paskaleva

5 – Increasing in importance

04. Those Charged With Governance

Kaori Ito (Yourmysyar Inc.)

5 – Increasing in importance

Technology-enabled financial crimes continue to increase in speed and sophistication, challenging traditional detection and control mechanisms. This trend highlights the importance of strengthening how professional judgment and ethical responsibility are exercised earlier in the risk lifecycle, before issues crystallize into clear breaches.

05. Regulators and Oversight Authorities

National Association of State Boards of Accountancy (NASBA)

5 – Increasing in importance

No matters to highlight at this time.

Public Accountants and Auditors Board Zimbabwe (PAABZ)

Over the past years, technology enabled financial crime in our jurisdiction has shifted from high volume and small value opportunistic hits to highly organized, high impact operations powered by artificial intelligence and digital asset exploitation. Despite the rising threat, majority of the entities in our jurisdiction lack adequate training and tools to handle modern cybercrime. This creates the need for a relook at the extent to which Risk assessment is performed on such areas. Given the sophistication of cybercrime, this brings ethical consideration on composition of the audit team as well as whether a client's IT infrastructure is actually auditable using firm existing tools. If the client's technology exceeds the firm's capacity, the standard should provide a clear off-ramp or mandatory requirement for specialist involvement.

5 – Increasing in importance

Tokyo Stock Exchange

5 – Increasing in importance

As stated in the response to A1.

06. Jurisdictional and National Standards Setters (JSS)

Auditing and Assurance Standards Board of Canada (AASBC)

- Focus on integrity and security: Fraud financial crime, and cyber security are top concerns across most entities in Canada and globally. For example, in the financial sector:
 - o the Office of the Superintendent of Financial Institutions (OSFI) identified "Integrity and security risk" as its leading priority for 2025–26 [<https://www.osfi-bsif.gc.ca/en/about-osfi/reports-publications/osfis-annual-risk-outlook-fiscal-year-2025-2026>], as heightened geopolitical tensions, rapid technological advancements, and increased reliance on a complex network of third parties have created vulnerabilities to the integrity and security of Canadian institutions and the financial system.
 - o The Canadian government is advancing a national Anti-Fraud Strategy and new Financial Crimes Agency, highlighting the growing importance of sovereign AI capabilities and their interconnection with banking obligations. These developments underscore the increasing interdependence between technology, financial institutions, and regulatory oversight in addressing technology-enabled fraud risks and protecting financial system users.

5 – Increasing in importance

GLASS Group of Latin American Accounting Standard Setters (GLENIF)

- The use of technology in business has increased the risk that organizational controls become vulnerable and fail to detect transactions that may constitute financial crimes. Greater emphasis should be placed on professional skepticism regarding the acceptance and continuation of work.
- We must emphasize the strengthening of ethics, because as the use of technology increases, so does the risk of digital crimes.
- Financial crimes facilitated by technology (digital fraud, money laundering with crypto assets, algorithmic manipulation, cyber fraud, financial deepfakes) will increase significantly and steadily.
- Because attacks and illegal activities will be detected.

5 – Increasing in importance

Hong Kong Institute of Certified Public Accountants (HKICPA)

5 – Increasing in importance

Hong Kong has seen a sharp rise in tech-enabled financial crimes – from sophisticated cyberattacks on banks to AI-driven fraud schemes. In 2025 alone, the HK Police handled ~19,000 cybercrime cases in the first 7 months (with losses over HK\$3.6 billion, up 18% YoY) and reported criminals using deepfakes and AI chatbots to perpetrate ransomware and scams. These developments reinforce the importance of understanding clients' IT environments and related controls when assessing audit risks and designing audit responses.

For the IAASB, existing standards already address fraud risk identification and understanding of IT environments. The focus for the next strategy period should therefore be on supporting consistent application of these standards, for example through non authoritative guidance or practical materials that help auditors understand how technology can both enable financial misconduct and affect risk assessment under standards such as ISA 250 (Revised) and ISA 315 (Revised 2019). More frequent and agile updates or implementation support may be needed in this area (e.g. practice alerts, Q&As or targeted enhancements), including continued attention to fraud-related requirements (e.g. ISA 240), given the pace of change in digital threats. For the IESBA, technology-enabled financial crimes raise questions about ongoing professional competence, due care and the handling of non-compliance with laws and regulations. The IESBA may wish to consider whether targeted implementation support is needed to help professional accountants stay alert to emerging forms of misconduct (e.g. deepfakes or AI-assisted scams), while reaffirming that the existing NOCLAR framework and ethical principles remain central and applicable in digital contexts.

07. Accounting Firms

Alan Am

5 – Increasing in importance

see above.

Deloitte Touch Tohmatsu Limited

IAASB – While we recognize that emerging technologies may alter the nature and complexity of financial crimes, we do not believe the auditor's responsibility has changed with respect to fraud and NOCLAR and that existing standards remain fit for purpose. We recommend the SSBs focus their efforts on developing guidance for applying existing standards to new technology-enabled fraud scenarios. For example, auditors would benefit from non-authoritative guidance/educational material on the application of professional skepticism in identifying and responding to risks associated with technology and cybercrime. The IAASB's Professional Skepticism Consultation Group could be a valuable source of input in this regard.

IESBA – We do not think this trend merits standard setting at the global level by IESBA. The fundamental principles of integrity and professional behavior in the existing Code are sufficient to address this topic. Any specific provisions are best addressed locally. We encourage IESBA to focus on the post-implementation

5 – Increasing in importance

Jack Schoeman (PWC)

5 – Increasing in importance

The main issue here is that certain financial crimes may be happening at a speed or complexity that traditional audit methods might not always detect. The SSBs' current standards were largely built for different systems and may not fully address the specific digital risks seen in the world today. We do not need more legislation or more layers of regulation that add complexity. Instead the boards should update existing standards to ensure auditors can better use modern data tools to identify potential risks. This is a practical way to modernize the SSBs' approach and help bridge the expectation gap on fraud while keeping the profession relevant to the public interest.

José María Hinojal (BNFIX)

5 – Increasing in importance

Kudos International

5 – Increasing in importance

This is an area that is changing all the time and is very difficult

Shreekant Prasad (Govindham Consultancy Services)

5 – Increasing in importance

08. Sustainability Assurance Providers other Than Accounting Firms

Anum Atique (Islamic Non Banking Financial Institution)

5 – Increasing in importance

The oversight ethics should be complied at the local regulations because the influence of the management always override the safety of the ethical code of conduct of the ethics Governance.

10. Member Bodies or Other Professional Accountancy Organizations

Association of Chartered Certified Accountants (ACCA)

5 – Increasing in importance

Technology-enabled financial crime is primarily addressed through regulatory and enforcement frameworks; however, it continues to have implications for audit, assurance, and ethics.

From an IAASB perspective, the increasing complexity of such risks may affect fraud risk assessment, audit procedures, and the exercise of professional scepticism. In a world driven by GenAI, and other emerging technologies, SSBs should consider implications for reliability and authenticity of audit evidence, particularly in relation to third-party sources.

The ISA 240 (Revised) has been recently revised with an effective date beginning on or after December 15, 2026. Given the pace of technological developments, a post implementation review of the standard would provide a useful mechanism to assess whether further enhancements are needed once it has been applied in practice for a few years.

Furthermore, in light of IAASB's ongoing on audit evidence standards (ISA 500 series), the Board should continue to monitor the technological developments and consider whether additional guidance is required to support consistent implementation.

From an IESBA perspective, evolving risks may raise considerations relating to integrity, professional behaviour, and the responsibilities of professional accountants in responding to potential non-compliance with laws and regulations, including in contexts where technology may facilitate or obscure such activities.

This trend is expected to increase in importance and evolving driver for both Boards in light of the rapid evolution in technology, requiring a combination of standard-setting, non-authoritative materials, and implementation support.

Belgian Institute of Tax Advisors and Accountants (ITAA)

Hacking and the security of our online data is a very big threat to our profession.

5 – Increasing in importance

Chartered Accountants Ireland (CAI)

5 – Increasing in importance

There is a strong link between this example and example A1, the increasing use of emerging technologies. The increase in financial crimes enabled by technology is recognised as a serious and growing concern globally. However, the primary responses to these risks lie within law enforcement, regulatory, supervisory and compliance frameworks, rather than ethics standard-setting.

From the perspective of professional ethics and auditing, the existing frameworks already address the core issues raised by technology-enabled financial crime. In particular, the Non-Compliance with Laws and Regulations (NOCLAR) provisions in the IESBA Code of Ethics establish clear responsibilities for professional accountants to respond appropriately to suspected or identified illegal acts in the public interest. Similarly, ISA 240, The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements,

explicitly addresses the risks of fraud, including those arising from the use of sophisticated tools and techniques, and reinforces the need for professional scepticism and vigilance.

If any further support is considered helpful, this would be best provided through application-focused guidance that reinforces how existing ethical and auditing requirements, such as NOCLAR and ISA 240, should be applied in technologically advanced environments, rather than through expanded or prescriptive standards.

Post-implementation reviews (PIR) should be treated as a core discipline that informs whether further standard setting is necessary, and a PIR of NOCLAR and ISA 240 with a view to identifying any gaps in the application of the principles and requirements would be useful.

Consejo General de Economistas de España

5 – Increasing in importance

SSBs:

The fight against money laundering and terrorist financing is part of the regulatory scope of each jurisdiction and the regulatory compliance that each company and professional must assume and that is included in the code of ethics. In addition, in many jurisdictions, auditing firms and accounting and tax services, as well as accountants, tax advisors and individual auditors are bound by specific anti-money laundering laws with their own obligations. These obligations should be proportionate to the size of the service provider and the risk of the entity/client, and should be part of the analysis of the acceptance of the engagement. Cybersecurity forces companies to increase the resources allocated to risks such as monetary fraud, information theft, unavailability of services, sabotage of infrastructures and loss of reputation. The probability and impact of these risks increases with the use of new technologies, therefore, SSBs should promote a preventive approach through the development of a global security strategy, security monitoring and surveillance, proactive threat management, coordination, dedicated and expert personnel and training and awareness of personnel. The auditor, accountants, and tax advisors must assess their cybersecurity risk. In the case of auditors, cybersecurity risk may require adapting NIGC 1. Cybersecurity should be treated as a matter of managing the quality, confidentiality and operational continuity of audit firms, not just as a technological risk. The non-binding guidance should address how firms, especially SMPs, should consider cybersecurity risks in customer acceptance and continuity, information protection, third-party vendors, access control, incidents, cloud tools, and quality management systems. systems.

European Federation of Accountants and Auditors for SMEs (EFAA)

5 – Increasing in importance

From an EFAA perspective, the rise of technology-enabled financial crime is clearly a cross-cutting risk trend that should be reflected in the agendas of the IAASB and IESBA.

The IAASB and IESBA should explicitly address risks arising from AI-enabled fraud, cyber-enabled manipulation of accounting records, digital evidence reliability, and professional reliance on automated tools. Particular attention should be given to the proportional impact on SMEs and SMPs, including practical guidance on fraud risk assessment, cyber controls, NOCLAR implications, and ethical use of AI in professional services.

Institute of Public Accountants (IPA)

5 – Increasing in importance

Given the different frameworks in each jurisdiction in dealing with financial crimes, IPA is of the view that addressing matters relating to financial crimes enabled by technology is a matter for each jurisdiction. As per our comment in A.1, any support to stakeholder by the SSB could be in form of guidance.

Polish Chamber of Statutory Auditors (PIBR)

5 – Increasing in importance

11. Academics

Kenichi Akiba (Waseda University)

5 – Increasing in importance

12. Others

Cristian Emmanuel Munarriz

5 – Increasing in importance

Louise Willdridge (LBW Global)

5 – Increasing in importance

Wai Man (Emily) Ho

5 – Increasing in importance

Wenzel Reyes (MindBridge)

5 – Increasing in importance

05.04. 6 – Strongly increasing in importance

02. Users of Financial or Non-Financial Information

CFA Institute

6 – Strongly increasing in importance

It appears that fabricating transactions and documentation for them has become very inexpensive, which could change the degree to which they can be relied upon as audit evidence (to the extent they are today).

Impax Asset Management

6 – Strongly increasing in importance

From Impax's standpoint, this trend warrants heightened attention because:

- Investors increasingly rely on auditors and assurance providers as part of the trust architecture underpinning capital markets.
- The intersection of technology, fraud, and weak governance can undermine confidence in both financial and sustainability reporting.
- Ethical expectations around competence, confidentiality, professional behavior and public interest responsibilities are becoming more critical.

Jane Wilson (Wilsojay Investments)

6 – Strongly increasing in importance

Well, I suppose you'll want to add another 10 pages to annual reports on a company's readiness for cyber war.

Jose Esposito (Credicorp Ltd.)

6 – Strongly increasing in importance

Koei Otaki (SMBC Nikko securities Inc)

6 – Strongly increasing in importance

The European Federation of Investors and Financial Services Users (BETTER FINANCE)

AI and digital systems can facilitate more sophisticated forms of fraud, manipulation and misconduct while also creating new vulnerabilities. These developments have direct implications for market confidence and investor protection. The SSBs should consider whether standards and related guidance sufficiently equip professionals to identify emerging risks and maintain professional skepticism in increasingly technology-driven environments. Strengthened engagement with cybersecurity, forensic and technology experts may also be appropriate.

6 – Strongly increasing in importance

03. Preparers or Issuers of Financial Statements or Other Information

Ajinomoto Co., Inc.

6 – Strongly increasing in importance

As technology advances and financial crime risks become more sophisticated, the importance of cybersecurity measures, internal controls, and information management is increasing for companies. In this environment, companies would welcome practical guidance from the SSBs on how corporate efforts and management frameworks should be assessed and incorporated in audit and assurance practice. For example, in the context of corporate cybersecurity efforts, we would like guidance or guidelines (without being prescriptive about the format) that clarify what kinds of KPIs should be used to assess performance—such as the level of implementation, adequacy, or maturity of cybersecurity measures.

Ascendia EOOD

6 – Strongly increasing in importance

05. Regulators and Oversight Authorities

Botswana Accountancy Oversight Authority (BAOA)

6 – Strongly increasing in importance

No matters or additional impacts to highlight.

Hellenic Accounting and Auditing Standards Oversight Board (HAASOB)

6 – Strongly increasing in importance

The nature of financial crime is rapidly evolving. Tackling these interconnected risks requires a proactive, collaborative approach between the public and private sectors. Track global guidelines and anti-money laundering strategies through the Financial Action Task Force is a way forward so auditors are aware of the dark web and digital assets ecosystems.

Independent Regulatory Board for Auditors (IRBA)

6 – Strongly increasing in importance

The growing sophistication of technology-enabled financial crime increases pressure on auditors to respond effectively to heightened fraud risks, cyber threats, and the manipulation of digital information. This trend amplifies expectations that standards clearly articulate how foundational requirements such as, risk assessment, audit evidence, documentation and professional scepticism apply in increasingly complex, data-driven environments. It also highlights the interconnected nature of audit and ethics considerations, particularly in relation to judgment, objectivity and accountability when technology is used to generate, process or validate information. A coordinated approach by the SSBs in monitoring emerging risks and responding through targeted enhancements or guidance would support more consistent and effective application globally.

Irish Auditing & Accounting Supervisory Authority (IAASA)

It may be beneficial to consider guidance on identifying (suspected) fraud and NOCLAR enabled by technology and appropriate responses to this risk in an audit.

6 – Strongly increasing in importance

UK Financial Reporting Council (UK FRC)

6 – Strongly increasing in importance

AI is increasingly facilitating scams and fraud, including through the use of 'deep fakes'. ISA 240 has only recently been revised and we do not suggest reopening it again at this time. However, we recommend the SSBs further explore the threats of financial crimes enabled by technology and whether guidance could be developed to assist professional accountants identify and address those threats.

06. Jurisdictional and National Standards Setters (JSS)

Brazil Institute of Independent Auditors (IBRACON)

6 – Strongly increasing in importance

Although there are several improvements resulting from ISA 240 revision, related to audit procedures that address risks of material misstatement due to fraud, including the use of technology to enhance audit procedures and considerations related to fraud schemes amplified by the use of technology, ISA 250, which deals specifically with noncompliance with laws and regulations, has opportunity for improvement on the requirements related specifically to financial crimes using emerging technologies, including audit procedures that the auditor can consider in these cases, for example, matters related to cybersecurity, general IT information and AI use in the preparation of financial information.

Instituto Mexicano de Contadores Públicos (IMCP)

6 – Strongly increasing in importance

Financial crime is a hot topic for Mexico as the regulators are focusing efforts on money laundry, tax evasion, bribery, corruption and digital impact related to fiscal and regulatory matters. Also, technology is evolving at a very rapid pace outdating the way auditors used to execute the audit work. Moreover, there is an increase in regulations, restrictions and even sanctions due to their pervasive effects. A project which encompasses the inclusion of technology in guidance or any other type of literature will be a benefit for practitioners because of the nature of the responsibilities of the assurance practitioners and the demand of the regulators to increase quality of the audits in respect of fraud or suspicious of fraud linked to financial crimes. Overreliance when using technology plus the automation of processes have an impact on ethics, professional scepticisms and judgements.

New Zealand Auditing and Assurance Standards Board (NZAuASB)

6 – Strongly increasing in importance

Cybersecurity continues to be a focus for a small economy such as New Zealand. We have seen increased incidents of hacking and phishing in the past few years. These attacks continue to increase in sophistication and are often sourced overseas and can lead to reduced access or no access to audit evidence or decreasing reliability of audit evidence.

Given the rise in technology-enabled financial crime, this is a good opportunity for the SSBs to clarify auditors' responsibilities in relation to non-compliance with laws and regulations for financial related crimes. As these crimes often originate in other jurisdictions, consistent international standards applied across the different jurisdictions are important.

Saudi Organization for Chartered and Professional Accountants (SOCPA)

6 – Strongly increasing in importance

07. Accounting Firms

AFCA Desarrollos Profesionales

El crecimiento de expertos informaticos que hacen mas complejo detectar los fraudes de manera preventiva.

6 – Strongly increasing in importance

Baker Tilly International

Auditors are perceived, rightly or wrongly, as being on the front line here so it is very important to manage what the auditor is required or able to do but also manage the public interest expectations.

6 – Strongly increasing in importance

BDO International Limited

6 – Strongly increasing in importance

The risk of Cybercrime increases as technology becomes more sophisticated, with perpetrators frequently finding new and different ways to commit crime.

As a result, agile, timely NAM is needed rather than setting new or revised standards. Producing NAM - aimed at protecting the public interest - would focus on the impact to a firm's system of quality management and to engagement teams as they consider the impact of the entity which is the subject of the engagement. Ethical considerations regarding technology also will need to be brought into play. This NAM should be developed jointly by IAASB and IESBA and in a way which avoids duplication of activities (i.e., by separately designed processes). As this is a dynamic and evolving area, we recommend that the process for this NAM starts during the current SWP period (perhaps as part of the Technology Quality Management Project) and is then reviewed and updated on a timely basis.

Grant Thornton International Ltd (GTI)

6 – Strongly increasing in importance

We agree that technology can increase opportunities for financial misconduct, including fraud. We strongly agree with the premise in the ISAs that auditors are not trained in document authentication and that document authentication is outside the scope of a financial statement audit. Although financial crimes and threats to cybersecurity continue to become more sophisticated, such threats are not new. In our view, ISA 240 (Revised) and the IESBA Code already provide principles-based requirements related to professional skepticism, fraud risk assessment, and responses to identified fraud risks, including risks related to authenticity. We are concerned further standard setting related to this matter could widen the expectations gap and that based on the standard-setting timeline, any such standards would not be effective in a timely manner to address such risks. Therefore, we recommend pursuing non-authoritative guidance instead of new requirements related to the impact of this trend on audit engagements. Non authoritative guidance should be educational in nature and provide example situations rather than prescriptive rules to follow.

We believe ISAE 3000 is sufficiently principles-based to accommodate the emergence of different types of assurance engagements listed above. We recommend the SSBs wait to develop entirely new standards for such engagements until the related geopolitical and regulatory landscape evolves sufficiently and the SSBs have completed robust outreach with relevant stakeholder groups.

Krzysztof Burnos

6 – Strongly increasing in importance

MAH, Chartered Accountants

6 – Strongly increasing in importance

We have audited some companies involved in crypto currencies/tokens and they can sometimes be so complicated that its possible auditors may not fully understand them or miss potential fraud. Some countries have strong controls or taxes over certain currency flows or transactions. So its possible that some companies could try to use digital assets to evade the controls and make illegal transfers.

08. Sustainability Assurance Providers other Than Accounting Firms

Keung Ho Keung Ricky

6 – Strongly increasing in importance

09. Public Sector Organizations

Audit Board of Republic Indonesia

6 – Strongly increasing in importance

Cybercrime is a massive and serious crime, therefore both SSBs should develop standard that will mitigate the challenges.

10. Member Bodies or Other Professional Accountancy Organizations

Asociación Interamericana de Contabilidad (AIC)

Los delitos financieros, son en base a plataformas y estrategias con inteligencia en "permanente actualización y creación".

6 – Strongly increasing in importance

Chamber of Hungarian Auditors (MKVK)

6 – Strongly increasing in importance

Development of guidance is important to increase awareness, prevent occurrence or address situation when the crime was identified.

Chartered Accountants Australia and New Zealand (CAANZ)

6 – Strongly increasing in importance

Regulation and enforcement in relation to technology-enabled financial crime sits outside the remit of the SSBs however the prevalence and increasing sophistication of these crimes does impact audit, assurance and ethics.

For the IAASB: Increases in hacking incidents will continue to present a risk. Firms need to consider and manage data privacy and cybersecurity risks as part of their quality management frameworks and overall risk management. Auditors need to be alert to the possibility of AI being used to fabricate documents that purport to be from third parties and support information in financial and sustainability reports. Auditors may need to place greater reliance on independent third-party data sources—such as direct confirmations—to validate evidence authenticity. This may challenge ISA 200.A24 "The auditor may accept records and documents as genuine unless the auditor has reason to believe the contrary." The IAASB will need to consider the impact of technology when it undertakes a PIR of the revised fraud standard and throughout the audit evidence and risk response and 500 series projects.

For the IESBA: Technology-enabled crimes may impact NOCLAR responsibilities. The board needs to consider the impact of emerging technologies on the fundamental principles of the Code.

We believe that in the absence of clear evidence of the need for a standard setting response, that the strategies of the SSBs should prioritise guidance to assist practitioners to apply the existing principles to emerging circumstances.

Pan African Federation of Accountants (PAFA)

6 – Strongly increasing in importance

The increasing use of emerging technologies has significantly amplified the scale, speed, and sophistication of financial crimes, including cyber fraud, digital laundering, and AI-enabled manipulation of financial systems. In Africa, this risk is compounded by varying levels of cybersecurity infrastructure, enforcement capacity, and digital literacy.

The IAASB and IESBA should strengthen their response by enhancing standards and guidance related to fraud detection, cybersecurity risk, and audit responses to technology-enabled misconduct. For IAASB, this includes clearer expectations on auditing in high-risk digital environments, evaluating IT controls, and applying professional skepticism when dealing with automated systems and complex data trails.

For IESBA, there is a need to deepen ethical requirements around confidentiality, integrity, and objectivity in environments exposed to cyber threats and financial crime risks, as well as guidance on professional conduct when dealing with suspicious digital transactions or compromised systems.

A key African priority is the need for capacity-sensitive implementation support, including practical tools and training for SMPs and regulators who may lack advanced forensic or cybersecurity capabilities.

Finally, both boards should strengthen collaboration with cybersecurity experts, regulators, and regional bodies to ensure standards remain responsive to rapidly evolving financial crime typologies and do not assume uniform global enforcement capacity.

Pavel Dimitrov (Union of Accountants in Bulgaria)

6 – Strongly increasing in importance

Technology-enabled financial crimes represent one of the most significant and rapidly escalating risks to financial integrity, public trust, and global market stability. The increasing use of AI, digital platforms, automated systems, and cross-border digital transactions requires strong, globally aligned standards to prevent misuse, ensure ethical conduct, and support effective oversight. A rating of 6 reflects the critical importance of addressing fraud, cyber-enabled financial manipulation, money laundering, and other technology-driven threats within the profession.

South African Institute of Chartered Accountants (SAICA)

6 – Strongly increasing in importance

SAICA acknowledges that attention should be given to AI governance, cybersecurity, fraud risk, and overreliance on automated tools. Cyber security breaches are a significant contributor to financial crimes. These crimes originate both from internal (modification of coding and/or unauthorized transactions through the unauthorized use of access privileges) and external sources (phishing, unauthorised remote access, leaked data available on the dark web, API vulnerabilities).

Financial crime is a matter of significant public interest and is subject to increasing scrutiny by regulators globally, including bodies such as the Financial Action Task Force (FATF). Given the role of audit practitioners as trust and company service providers (TCSPs), and their proximity to the establishment of legal entities as well as oversight of financial information, there is a growing expectation that the profession should play a more prominent role in the prevention and detection of money laundering and other financial crimes.

This was evident in South Africa following the country's inclusion on the FATF grey list, where TCSPs (including those providing auditing services) were designated as accountable institutions under recently promulgated legislation aimed at combating financial crime.

While emerging and enabling technologies used by reporting entities may increase the risk of misuse for illicit purposes, the varying levels of regulatory maturity across jurisdictions necessitate a cautious and measured response by the SSBs.

SAICA is of the view that adequate research should be undertaken to clearly identify the areas where standard setting intervention or guidance would add value. Therefore, during the 2028-2031, the SSBs could focus on extensive research rather than looking to produce guidance or standards. Constructive engagement with FATF, national regulators, financial reporting standard setters and other relevant global bodies could assist in clarifying expectations, identifying gaps, and determining the appropriate role for the Boards without inadvertently extending responsibilities beyond their intended remit. Ultimately, any standard setting intervention in this area would need to be part of a jurisdictional regulatory framework.

11. Academics

European Accounting Association (EAA) Auditing, Assurance and Ethics Standard Committee

The Committee would like to draw attention on the role of AI in the context of fraud risk. As AI continues to evolve and its use in financial reporting and control environments expands, emerging fraud typologies and data governance expectations will require continued attention. In this regard, the Committee encourages both IAASB and IESBA to monitor developments in this area as experience grows, ensuring that standards remain fit for purpose in increasingly AI-driven contexts. The Committee further encourages close coordination to ensure consistency.

6 – Strongly increasing in importance

Kiran Seth (Sunway University)

6 – Strongly increasing in importance

with the passage of time, there will be higher rates of crimes by technology

Nicole Ratzinger-Sakel (University of Hamburg Business School)

6 – Strongly increasing in importance

12. Others

AIDS Committee of Toronto

6 – Strongly increasing in importance

We need to stay ahead of the curve as fraudsters always seem to be at least one step ahead.

Kazuhiro Yoshii (Securities Firm)

6 – Strongly increasing in importance

Mahmoud Bilal (Unimar)

6 – Strongly increasing in importance

05.05. Letters providing separate ratings for IAASB or IESBA

06. Jurisdictional and National Standards Setters (JSS)

Accounting Professional & Ethical Standards Board (APESB)

5 – Increasing in importance

Matters relating to IESBA:

APESB considers that emerging technologies are accelerating both the scale and sophistication of financial misconduct, creating new challenges for practitioners applying the Code's fundamental principles and independence requirements. For example, artificial intelligence (AI) is now being used to generate fraudulent documentation, including in mortgage applications. These developments reinforce the need for the Code to provide clear expectations regarding professional scepticism, the evaluation of information produced by automated systems and the ethical responsibilities of practitioners when confronted with technology-enabled fraud.

Technology-enabled financial crime also intersects with issues of data integrity and transparency. The increasing prevalence of complex or opaque ("black box") systems means that practitioners Joint IESBA and IAASB Stakeholder Survey Strategy and Workplans for 2028-2031 may have limited visibility into how information is generated or manipulated. This raises ethical considerations related to competence, due care, and the obligation to obtain sufficient understanding of the systems and data relied upon in professional activities.

APESB also notes that this issue is highly jurisdiction-specific and shaped by local legislation and enforcement frameworks. APESB recommends that IESBA consider whether any work beyond the existing NOCLAR provisions in the Code is needed in this area.

American Institute of Certified Public Accountants - Professional Ethics Executive Committee and Auditing Standards Board (AICPA PEEC & AICPA ASB)

IESBA and IAASB rating: 4

Though this is an important global trend that warrants SSB monitoring, we believe existing principles-based requirements in extant standards are fit for purpose.

The IESBA code addresses fraud through two complementary mechanisms. First, the NOCLAR provisions equip professional accountants to respond appropriately to actual or suspected noncompliance. Second, and more fundamentally, the principles of integrity and professional behavior establish enforceable ethical expectations that operate as a strong deterrent against engaging in or enabling fraudulent conduct. These principles shape professional judgment and behavior ex ante, influencing decision-making before misconduct occurs and reinforcing accountability through ethical obligations, disciplinary mechanisms, and reputational consequences. Taken together, these mechanisms create a framework that supports fraud prevention in a manner that is scalable, globally applicable, and resistant to rapid obsolescence, suggesting that further prescriptive intervention by IESBA in this area would yield diminishing returns relative to other priority areas.

Similarly, existing IAASB standards, including ISA 240 and ISA 250, provide an appropriate foundation for auditors and practitioners dealing with these topics. However, nonauthoritative material developed by the SSBs may be used to address the implications of AI (e.g., fake authorization, deepfakes). For example, IESBA could consider whether focused educational material would be helpful in supporting professional accountants' awareness of new and evolving forms of financial crimes, such as AI-enabled fraud, while underscoring that the existing NOCLAR framework and core ethical principles continue to be relevant and effective in digital environments. In doing so, IESBA could explore opportunities to collaborate with other stakeholders actively engaged in this area and coordinate with the IAASB to help mitigate the impact of limited resources.

4 – Slightly increasing in importance

Australian Auditing and Assurance Standards Board (AUASB)

– Strongly increasing in importance

6

Technology is expected to make financial crime increasingly complex and widespread by lowering barriers to entry and eroding jurisdictional boundaries, facilitating falsification of documents and other evidence, thereby enabling criminal activity to be conducted more easily, anonymously and across borders at scale. The reliability of audit evidence is crucial for assurance providers. We recognise the importance of the revisions to ISA 500 when considering the reliability of audit evidence. We acknowledge that the draft of ISA 500 recognises that authenticity is one attribute of reliability of information that may or may not be significant in the circumstances to meet the intended purpose(s) of an audit procedure and that auditor judgement is needed to determine the nature and extent of testing authenticity of information.

[Institut der Wirtschaftsprüfer \(IDW\)](#)

5 – Increasing in importance

IAASB

Financial crime is becoming a higher priority as advances in artificial intelligence are lowering the barriers to sophisticated fraud. Tools such as deepfakes and AI-generated documents make it easier to impersonate individuals and bypass traditional controls, while AI also enables users to circumvent IT security measures with greater confidence and precision. At the same time, increasing digitalization heightens exposure to cybersecurity threats, as weaknesses in systems can be exploited to gain unauthorized access, manipulate data, or facilitate fraudulent activities. Together, these developments increase both the scale and complexity

of financial crime risks, challenging existing control frameworks. For these reasons, we believe that financial crime in conjunction with artificial intelligence ought to be an area of focus for the IAASB both in terms of applying existing standards and recognizing the inherent limitations of audits and other assurance engagements in this area.

IESBA

We believe that the Code already offers a robust, principles-based framework that remains suitable for purpose in relation to financial crimes through technology. The IESBA's value-add is not to replicate or broaden fraud-focused requirements, but to maintain confidence that the Code continues to address evolving risks as technology changes how misconduct may be perpetrated or concealed.

Nordic Federation of Public Accountants (NRF)

3 – Slightly decreasing in importance

We acknowledge the increase in financial crimes in society, not least driven by the growing use of technology and AI. Recent revisions to ISA 240 have already sought to strengthen the auditor's responsibilities in this area, and the extensive anti money laundering regulatory frameworks in many jurisdictions also address these risks. From our perspective, these developments suggest that further changes to the standards are not the immediate priority.

At the same time, the rise in financial crime may lead to increased demand for external assurance services beyond the audit. Should such needs emerge, any initiative from the IAASB should take ISAE 3000 as the starting point, ensuring a consistent and principles based foundation for any future work.

With respect to the Code, and consistent with our responses to other questions, we believe that the fundamental principles are robust enough to be applied to these situations as well. Given the rapid pace of change — where it is difficult to anticipate what new forms of financial crime or technology enabled misconduct may arise over the next five years — it is reasonable to expect

that new scenarios will emerge. However, such developments should primarily be addressed through non-authoritative material, which provides the necessary agility without compromising the stability and principles based nature of the Code.

07. Accounting Firms

Ernst & Young Global Limited (EY)

6 – Strongly increasing in importance

Our impact rating for this trend is based on our considerations for the IAASB. With regard to the IESBA, we believe the impact rating would be 4 (Slightly increasing in importance).

The following paragraphs provide further recommendations specific to each Board:

IAASB matters

Cyber incidents continue to threaten confidence in the financial reporting ecosystem and the frequency and sophistication of

attacks against businesses and critical infrastructure are accelerating. This rapid evolution underscores the need for agility in the issuance of NAM to support auditors and practitioners. At the same time, emerging technologies and platforms are converging in ways that further heighten risk, including:

- Proliferation of AI technologies: Historically, financial crime required significant technical skill. Today, AI can supply that expertise, enabling attacks through deepfake driven fraudulent transactions and AI tools capable of breaking security or authentication protocols or identifying and exposing cyber vulnerabilities (e.g., Project Glasswing).

- Advancements in quantum technology: As quantum computing progresses, traditional cryptography will face increasing vulnerability. This may erode trust in digital infrastructure by enabling mass decryption of compromised data, weakening the deterrent effect of encryption in ransomware scenarios, and undermining digital authentication through more sophisticated impersonation techniques.
 - Information distortion through social platforms: Heavy reliance on social media as an information source increases the risk of human error as decisions may be influenced by disinformation. We observe that many major breaches still originate from mistakes made by help desk or support personnel inadvertently opening a pathway for attackers.
- Additionally, rising geoeconomic tension and political instability further intensify the cybersecurity landscape. Significant cyber breaches will also likely lead stakeholders to question the various roles within the financial reporting ecosystem and the responsibilities relating to cyber risk and cybersecurity in an audit of financial statements. As a response, we believe it would be beneficial for the IAASB to develop NAM to explain the auditor's responsibilities when assessing cybersecurity within a financial statement audit under its existing standards, including newly revised ISA 240.

Outside of audit, we are observing that escalating concerns over cyber risk, which are further amplified by the proliferation of AI, are driving increased demand for cybersecurity related attestations. In practice, we are seeing request for a broad range of such engagements, including program and control assessments, regulatory readiness and attestation, incident response simulations, International Organization for Standardization (ISO) certifications, and "shadow" breach investigations. Requests for these services are often driven by those charged with governance. Consistent with our comments on non-audit assurance related to digital assets, we believe there is value in continued consideration of how existing assurance standards can be applied more consistently to cybersecurity. Timely, topic specific NAM could assist in promoting clarity, consistency, and user understanding in this evolving area.

IESBA matters

As noted in our response to question A.1, we believe that the fundamental principles in the IESBA Code are already robust and sufficiently comprehensive to address ethical considerations arising from the growing use of emerging technologies, including cybersecurity threats and technology enabled financial misconduct. However, IESBA could consider using NAM to demonstrate how the IESBA Code applies in different situations. This approach would also allow the Board to address emerging issues in an agile and timely manner.

KPMG International Limited

IAASB – 4 Slightly increasing in importance, IESBA – 2 Decreasing in importance

We consider that the trend of "Financial Crimes Enabled by Technology" will slightly increase in importance over the survey period for IAASB's strategic planning, but decrease in importance in shaping the IESBA's planning. Advances in AI-enabled technology and quantum computing, in particular, have the potential to increase the scale and sophistication of certain types of fraud and financial crime. However, in relative terms, we believe this trend is likely to increase only modestly as a strategic driver for the IAASB because we consider that the primary risks entities face in respect of fraud and financial crime are mutating, rather than increasing overall, as follows:

- "Traditional" fraud risks arising from the ability of an entity's personnel to manipulate records in order to perpetrate fraud are reducing, given that, in respect of major networks, fraudulent transactions will be significantly more difficult to perpetrate unless there is a high degree of collusion across multiple entities. Furthermore, such infrastructure may provide a robust audit trail, with enhanced transparency regarding transactions, and immutable records, as compared to individual entity-based systems involving mainly bilateral transactions, and for which the audit trail may be paper-based. (However, we highlight that this is not always the case, in particular, in respect of less established networks, which may have higher validator/miner concentration and a less decentralized ecosystem);
- However, risks regarding unauthorized access by third parties to an entity's IT systems in order to commit fraud are increasing, as technological capabilities evolve, particularly in the area of quantum computing, and have the potential to significantly reduce/overcome the effectiveness of an entity's IT controls (such as controls over access to systems, e.g., password security). Furthermore, when such frauds do occur, they

are increasingly likely to be in the form of more serious financial crime perpetrated by organized criminals and which are likely to be of significantly greater impact to entities.

We highlight that the evolving risks in respect of fraud and financial crime, with digital infrastructure reducing the likelihood of occurrence of "traditional" frauds but also increasing the magnitude of the consequences of fraud/financial crime when it does occur, has significant implications for the ability of entities to prevent such events, as well as how auditors address associated risks when performing audit (or assurance) engagements. This changing landscape may contribute to an increase in the "expectation gap" in terms of stakeholders' expectations regarding the role and responsibilities of auditors to detect fraud and financial crime, and their professional responsibilities as set out in existing standards.

IAASB

We consider that, overall, the IAASB's standards are clear regarding the auditor's and assurance practitioner's responsibilities relating to fraud and non-compliance with laws and regulations, including, where applicable, financial crime.

However, we believe that the IAASB has an important role to play in convening discussions of key stakeholders, including entities, regulators, jurisdictional standard-setters, practitioners and others, in order to frame the debate regarding the relative roles and responsibilities of all parties within the financial reporting ecosystem. We also recommend that the IAASB liaise with IFAC to develop educational materials to help clarify the role and responsibilities of auditors in this evolving environment.

We consider that cybersecurity risks will remain ever-present, and while these can be monitored and mitigated by entities, e.g., by introducing enhanced controls that focus on security and safeguarding measures, such as key encryption and access protocols, they cannot be completely eliminated. In the current environment the risk of cyber-attacks on entities continues to increase, which, as demonstrated by recent, high-profile attacks on a number of entities across different jurisdictions, may have significant consequences for an entity and, in severe cases, may even impact an entity's ability to continue as a going concern.

We recommend that the IAASB monitor the ongoing evolution of technological developments, and the resulting impacts on audits, with a view to developing guidance in respect of how risks of technology-enabled fraud and financial crime may be considered and addressed as part of an audit. As discussed elsewhere in our response, we consider that the issuance of non authoritative guidance that can be developed rapidly, targeted at specific areas of auditor concern, and which can explore such matters in greater depth, is preferable to making incremental changes to the standards themselves.

IESBA

In the context of the IESBA's overall priorities, this trend is of lower relative importance. Existing principles based standards already provide a robust framework from an ethics and independence perspective for addressing threats arising from technology-enabled financial crimes.

Technology enabled financial crime is an emerging risk, with AI increasing the scale and sophistication of certain types of misconduct. These developments have contributed to a growing expectation gap between what stakeholders increasingly expect in AI enabled environments and the principles-based professional responsibilities defined in existing standards, which focus on judgment, accountability, and ethical behavior rather than outcomes.

The primary need in this area is therefore clarification and communication, including to demonstrate how existing principles in the Code apply in AI-enabled environments. This would help manage expectations about the role and responsibilities of professional accountants, rather than introducing changes to the Code itself.

4 – Slightly increasing in importance

09. Public Sector Organizations

United States Government Accountability Office (GOA)

4 – Slightly increasing in importance

We believe that ISA 240 and ISA 250 are sufficient to detail a practitioner's responsibilities for identifying, communicating, and reporting on fraud and noncompliance with laws and regulations related to financial misconduct, including those perpetrated by technology. We believe that the SSBs should continue to monitor and discuss technological developments, but we note that practitioners are not normally trained experts in detecting sophisticated financial crimes.

10. Member Bodies or Other Professional Accountancy Organizations

Accountancy Europe (AE)

5 – Increasing in importance

The increase in financial crime enabled by technology, including cyber-related risks is acknowledged. However, we consider that this issue is being framed in a way that overextends the role of standard setters. Financial crime is fundamentally a matter for legal and regulatory frameworks, including Anti-Money Laundering (AML) systems and enforcement mechanisms. In the European Union (EU), the new AML Regulation and 6th AML Directive are being implemented and the new EU wide regulator, AMLA, has started work.

While evolving risks such as cyber threats may increase expectations on auditors, particularly in areas such as risk assessment and going concern, this does not in itself justify the development of new auditing or ethical standards. Existing frameworks are designed to be adaptable to emerging risks, and the appropriate response should primarily involve guidance, supervisory focus and practical implementation support. However, more and better collaborations between AML experts and standard setters might need to be envisioned. IAASB rating: 5 Increasing in importance

IESBA rating: 2 Decreasing in importance

Global Accountancy Alliance (GAA)

6 – Strongly increasing in importance

IAASB Rating: 6

Financial crime is becoming a higher priority as advances in artificial intelligence are lowering the barriers to sophisticated fraud. Tools such as deepfakes and AI-generated documents make it easier to impersonate individuals and bypass traditional controls, while AI also enables users to circumvent IT security measures with greater confidence and precision. At the same time, increasing digitalization heightens exposure to cybersecurity threats, as weaknesses in systems can be exploited to gain unauthorized access, manipulate data, or facilitate fraudulent activities. Together, these developments increase both the scale and complexity of financial crime risks, challenging existing control frameworks. That said, IAASB standards, including ISA 240 and ISA 250, provide an appropriate foundation for auditors and practitioners dealing with these topics. In our view, existing standards are responsive to this topic. However, non-authoritative material developed by the SSBs may be used to address the implications of AI (e.g., fake authorization, deepfake).

IESBA Rating: 3

This is an important global development, but we expect it to become less of a strategic differentiator for the IESBA because the Code already offers a robust, principles-based framework that remains suitable for purpose. The Code supports deterring and addressing fraudulent conduct in two interrelated ways. First, the fundamental principles—particularly integrity and professional behavior—set enforceable expectations that help prevent professional accountants from participating in, facilitating, or disregarding fraudulent activity. These principles shape conduct upfront and are reinforced through professional obligations, disciplinary consequences, and reputational considerations. Second, the NOCLAR provisions

provide a structured basis for professional accountants in business and in public practice to respond appropriately to identified or suspected non-compliance with laws and regulations, including matters involving financial crime. We note that the post-implementation review of the NOCLAR standard is currently underway, and we intend to participate in that work.

Overall, this combination provides an approach to fraud prevention and response that is scalable, internationally applicable, and less likely to become outdated quickly—so additional prescriptive standard-setting in this area may deliver limited incremental benefit compared with other priorities. Separately, there may be scope for the IESBA to encourage jurisdictions to establish effective whistleblower protections, so that professional accountants (and others) who judge it necessary to raise concerns can do so with appropriate safeguards. We also understand the IESBA intends to develop further technology-related materials. Those resources will be most helpful where they translate the Code into practical, real-world examples that reflect challenges faced by professional accountants in business and in public practice. For instance, the recent IESBA podcast on quantum computing underscored that new technologies may increase the magnitude of existing threats, even where they do not necessarily introduce new categories of threats.

We again encourage the SSBs to work closely together on their respective technology-related work, given the significant overlap between ethics and assurance in this area. In that regard, because we see this as a higher priority for the IAASB, the IESBA may also need to adjust its priorities during the 2028-2031 workplan if the IAASB proceeds past monitoring of the trend and there is an ethical risk that must also be addressed.

Institute of Chartered Accountants in England and Wales (ICAEW)

4 – Slightly increasing in importance

ICAEW notes the increasing sophistication of AI systems which can be used to exploit system vulnerabilities to facilitate cyber crime. However, it is difficult to see how SSBs can produce global standards in this area, particularly given the speed at which the technology is evolving.

In the UK, financial crime is fundamentally a matter for legal and regulatory frameworks, including those introduced by the Economic Crime and Corporate Transparency Act 2023 which introduced a new offence of failure to prevent fraud; general Anti Money Laundering legislation and enforcement mechanisms.

In audit, extant ISAs such as ISA 240 and ISA 500 are sufficiently principles-based to allow practitioners to address the risks, alongside guidance from regulators and PAOs. Responsibility for prevention and detection of cyber crime should rest with company directors.

IAASB rating: 4

IESBA rating: 2

Institute of Chartered Accountants of Scotland (ICAS)

IESBA – Rating - 3

This is an important global development, but the IESBA Code already provides a durable, principles-based framework through the fundamental principles and NOCLAR, and any further materials should focus on practical application, with continued coordination between the SSBs on technology-related work in this area. There may be a role for IESBA to produce non-authoritative material to illustrate how the Code already effectively deals with such matters and to highlight the potentially increased level of threat that may be present. We note that a key message in the recent excellent IESBA podcast on quantum computing was that such technology will amplify the level of threat but is unlikely to create any new threats.

We also note that IESBA is looking to produce new guidance on technology. This is most useful where it clearly illustrates how the Code effectively deals with the real-life scenarios being experienced by professional accountants, both in business and in practice. This can be really useful for professional accountants in their day-to-day roles.

IAASB – Rating – 6

Financial crime risk is rising as AI and other technologies have enhanced the ability of bad actors to impersonate individuals, circumvent controls and hence commit more sophisticated fraud, including cyber fraud. Even so, existing IAASB standards, including ISA 240 and ISA 250, provide an appropriate foundation for auditors to undertake their work in these areas. In our view, any further response by the IAASB should consider the potential need for non-authoritative material addressing the implications of deepfakes and related threats.

6 – Strongly increasing in importance

International Federation of Accountants (IFAC)

IFAC acknowledges that financial crimes enabled by technology are an important public-interest concern. However, the implications for the SSBs are unclear. This is a very broad topic, and further detail is needed to understand the relevance of this trend specifically to either IESBA or IAASB. It should also be noted that recent revisions to ISA 240 have already sought to strengthen the auditor's responsibilities in this area, and that extensive AML and other legal or regulatory frameworks exist in many jurisdictions to address risks in this area. The implications may also differ significantly between the IAASB and IESBA. The issue may have clearer implications for the IAASB in relation to audit evidence, risk assessment, audit processes and client processes, but much less obvious relevance for IESBA.

For the IAASB, the relevant issue is not preventing technology-enabled financial crime but clarifying how existing audit and assurance standards apply when such risks affect the entity, the audit, audit evidence or risk assessment. Risks could include misuse of AI by fraudsters, management or auditors, and examples such as fake invoices or deepfake evidence. However, existing ISAs already allow such matters to be addressed, which points to the need for gap analysis before any standard-setting response.

For IESBA, there needs to be caution before concluding that new ethics or independence requirements are needed. Existing principles should first be considered.

IFAC therefore encourages monitoring, clarification, education and targeted non-authoritative material before any standard setting is considered. The SSBs should define the specific issue, identify which Board is affected, assess whether existing standards already address the matter, and avoid expanding auditor or professional accountant responsibilities into areas more appropriately addressed by management, those charged with governance, law enforcement, regulators or jurisdictional authorities.

– Slightly increasing in importance

4

05.06. No rating provided but with comments

01. Monitoring Group

International Federation of Independent Audit Regulators (IFIAR)

Financial Crimes Enabled by Technology

23. Increasing reliance on digital systems heightens risks related to data integrity, confidentiality, and cyber resilience. Practical guidance could assist auditors in appropriately considering these risks.

International Organization of Securities Commissions (IOSCO) Committee

A.3 Financial Crimes Enabled by Technology – High Influence

As part of the broader trend of increasing use of emerging technologies (see A.1), we also recognize that financial crimes enabled by technology may present a growing challenge for auditors, as digital information becomes more difficult to authenticate and new ways of perpetrating fraud continue to emerge. These developments have implications for how auditors identify, assess, and respond to risks of material

misstatement, including risks related to fraud, and underscore the importance of maintaining an appropriately high level of professional skepticism. As this trend evolves, we encourage the Boards to consider whether any issues arising from technology-enabled financial crimes indicate a need for further clarification within the existing standards or additional forms of support. In making such assessments, the Boards may benefit from insights gained through ongoing technology-related initiatives and engagement with other regulators and standard-setters to deepen their understanding of evolving risks and practical challenges in this area.

05. Regulators and Oversight Authorities

Committee of European Auditing Oversight Bodies (CEAOB)

11. Similarly, technology-enabled financial crimes pose growing challenges for society and auditors. This trend affects how auditors identify and respond to risks of material misstatement and reinforces the need for strong professional skepticism. As risks evolve, the SSBs may need to consider whether further clarification within the existing standards or additional support is warranted, informed by insights from ongoing technology initiatives and engagement with regulators and other stakeholders.

10. Member Bodies or Other Professional Accountancy Organizations

CPA Australia

A.3 Technology-enabled financial crime and cybersecurity:

Recognise as highly relevant to practice, but largely addressed through existing responsibilities and jurisdictional law/enforcement. SSBs should avoid scope expansion. For the IAASB, allow recent revisions (e.g., fraud-related) to bed down and support consistent application through implementation support and practice alerts rather than further standard-setting. For the IESBA, anchor responses in fundamental principles and NoCLAR (including PIR outcomes), with education/clarification where needed; primary solutions remain jurisdictional.

0– I do not agree that this is a trend to be considered

05.07. No specific response

02. Users of Financial or Non-Financial Information

First Nations Financial Management Board

Sarasin & Partners

03. Preparers or Issuers of Financial Statements or Other Information

Japan Business Federation – Keidanren

05. Regulators and Oversight Authorities

Canadian Public Accountability Board (CPAB)

Public Company Accounting Oversight Board (PCAOB) – Views of the PCAOB Chief Auditor