



IESBA™

International Ethics Standards Board for Accountants

AN IFEA BOARD

EMERGING TECHNOLOGIES

A Characteristics-Based Approach to Ethical Considerations for Professional Accountants

JULY 2026



IESBATM

International Ethics Standards Board for Accountants

AN IFEA BOARD

Key Contacts:

Ken Siong, IESBA Program and Senior Director (kensiong@ethicsboard.org)

Rui Peres Jorge, Director – Strategy and Communications (ruiperesjorge@ethicsboard.org)

Jeanne Viljoen, IESBA Principal (jeanneviljoen@ethicsboard.org)

Greg Walters, IESBA Senior Manager (gregwalters@ethicsboard.org)

About IESBA

The International Ethics Standards Board for Accountants® (IESBA®) is an independent global standard-setting board. The IESBA's mission is to serve the public interest by setting high-quality, international ethics (including independence) standards as a cornerstone to ethical behavior in business and organizations and to public trust in financial and non-financial information that is fundamental to the proper functioning and sustainability of organizations, financial markets and economies worldwide.

Along with the International Auditing and Assurance Standards Board® (IAASB®), the IESBA is part of the International Foundation for Ethics and Audit™ (IFEATM). The Public Interest Oversight Board (PIOB) oversees IESBA and IAASB activities and the public interest responsiveness of the standards.

Through intellectual property and service level agreements, the International Federation of Accountants® (IFAC®) manages requests to translate or reproduce IAASB and IESBA content. For permission to reproduce or translate this or any other publication or for information about intellectual property matters, please visit [Permissions](#) or contact Permissions@ifac.org.

The IESBA, IFEA and IFAC do not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

CONTENTS

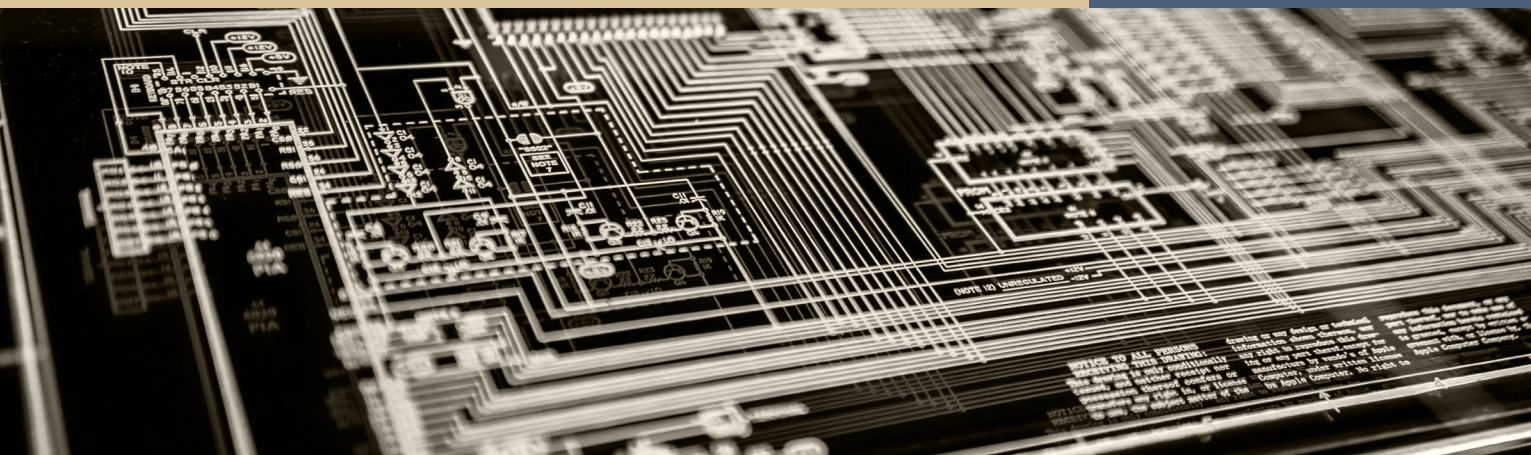
A. Introduction	4
B. Characteristics Associated with Emerging Technologies	6
C. Key Ethical Considerations	8
D. Conclusion	12
Appendix 1	13
Appendix 2	14

This publication has been prepared by the Staff of the [International Ethics Standards Board for Accountants](#) (IESBA). It highlights a number of important ethics and independence considerations for professional accountants in public practice (PAPPs) and professional accountants in business (PAIBs), under the [International Code of Ethics for Professional Accountants \(including International Independence Standards\)](#) (the Code¹) as they develop, implement or use emerging technologies.

This publication may also be of interest to regulators and audit oversight bodies, jurisdictional standard setters (JSS), professional accountancy organizations (PAOs) and others.

This publication does not amend or override the Code, the text of which alone is authoritative. Reading this publication is not a substitute for reading the Code. The guidance in the publication is not meant to be exhaustive and reference to the Code should always be made. This publication does not constitute an authoritative or official pronouncement of the IESBA.

¹ References to the Code in this publication are to the 2025 version of the Code incorporating approved pronouncements effective in December 2026, i.e., [Sustainability](#) and [Using the Work of an External Expert](#), except where otherwise stated.



A. INTRODUCTION

1. Technology continues to reshape how organizations operate, deliver value, identify and manage risks. Advances in areas such as artificial intelligence (AI), distributed ledger technologies, and advanced data analytics are accelerating decision-making and transforming traditional workflows.
2. While rules-based technologies² have long been used by professional accountants (PAs), emerging technologies³ increasingly exhibit characteristics – for instance opacity, non-determinism, perpetual adaptivity, and autonomy – that differ fundamentally from rules-based technologies. Enabled by significant advances in computing power over the last decade, these technologies now operate at a scale and speed that challenge human oversight, requiring PAs to develop a deeper understanding of how such characteristics affect their professional and ethical responsibilities.⁴
3. As emerging technologies evolve⁵, they introduce not only efficiencies and innovations, but also new challenges related to ethics, governance⁶, security, human oversight and accountability. The use of emerging technologies may give rise to circumstances that create or amplify threats⁷ to compliance with the fundamental principles⁸ of the [International Code of Ethics for Professional Accountants \(including International Independence Standards\)](#) (the Code).

-
- 2 Rules-based technologies are systems that use predefined “if-then” rules to make decisions, solve problems and automate reasoning in a transparent and interpretable manner.
 - 3 This publication uses the term “emerging technologies” to refer to new or rapidly evolving computer software and/or hardware technologies that are not yet fully mature, standardized, or widely adopted.
 - 4 For firms and PAs that perform audits and other assurance engagements, these technologies also have implications for their quality management responsibilities at the firm and engagement levels. The International Auditing and Assurance Standards Board (IAASB) has established a [Technology Quality Management \(QM\) Workstream](#) to develop non-authoritative material that clarifies and supports the consistent and effective application of the IAASB’s QM standards in circumstances where technological tools enabled by emerging technologies are used in engagements (see [Workstream Action Plan \(March 2026\)](#)).
 - 5 These technologies move at different speeds along the maturity curve. Some remain experimental, while others are rapidly becoming embedded in core operations.
 - 6 Effective organizational governance enhances compliance with the Code, including through controls over the identification and use of technologies, oversight of data quality, and mechanisms to ensure meaningful human review of outputs.
 - 7 Threats to compliance with the fundamental principles fall into one or more of the following categories: self-interest, self-review, advocacy, familiarity or intimidation (paragraph 120.6 A3 of the Code).
 - 8 The five fundamental principles are integrity, objectivity, professional competence and due care, confidentiality, and professional behavior (paragraph 110.1 A1).

4. The IESBA's 2023 [Technology-related Revisions](#)⁹, which became effective in December 2024, strengthened the Code and expanded its relevance vis-à-vis rapidly advancing technology. This publication highlights key ethical considerations under the Code to assist PAs in complying with the fundamental principles when they use emerging technologies. It is not intended to be a comprehensive analysis of all the ethical issues that might arise in practice.
5. The publication focuses on how the use of emerging technologies may create or amplify threats to such compliance because of the common characteristics associated with such technologies. This approach recognizes that while emerging technologies evolve rapidly, the characteristics associated with such technologies that are relevant in considering ethical risks remain relatively consistent over time.
6. By focusing guidance on these characteristics rather than on specific technologies or situations, the publication is intended to remain durable and have broad applicability in supporting PAs across a wide range of technologies and contexts. The IESBA will complement this publication with subsequent technology-specific guidance.

The Technology-Related Revisions

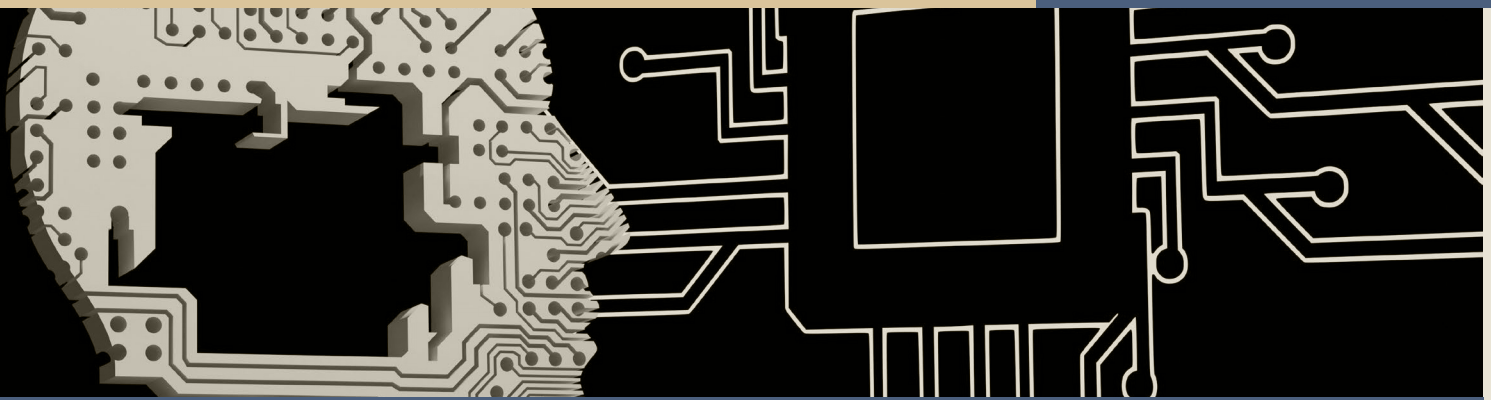
- » Strengthened the Code in guiding the mindset and behavior of PAs when they use technology.
- » Introduced enhanced provisions fit for the digital age in relation to the fundamental principles of confidentiality, and professional competence and due care, as well as in dealing with circumstances of complexity.
- » Strengthened and clarified the International Independence Standards by addressing the circumstances in which firms and network firms may or may not provide a technology-related non-assurance service to an audit or assurance client.



The technology-specific guidance to be developed by the IAASB may also be of relevance, owing to the complementary and mutually reinforcing nature of ethical and independence considerations under the IESBA Code and quality management considerations under the IAASB's QM standards.¹⁰

⁹ All relevant information concerning the technology-related revisions to the Code can be found on the [IESBA Technology Focus Page](#).

¹⁰ This may be particularly relevant for firms and PAs that perform audits and other assurance engagements. The IAASB's planned Technology QM guide series will specifically focus on Gen AI-enabled technological tools that are used in engagements.



B. CHARACTERISTICS ASSOCIATED WITH EMERGING TECHNOLOGIES

7. In the last decade, significant advances in computing power have enabled technologies to be deployed at scale and speed, and expanded the range and capabilities of tools available to PAs. However, these advances have also fundamentally altered the risk profile of such technologies, whose characteristics present new challenges for compliance with the fundamental principles of the Code.
8. Emerging technologies may exhibit certain specific characteristics, including:¹¹
 - **Opacity**, which may limit transparency and explainability, making it more difficult to identify biases, errors, or inappropriate assumptions embedded within the system (“black-box” behavior).
 - **Non-determinism**, where similar or identical inputs may produce different results.
 - **Dependence on data**, the quality, completeness and relevance of which directly influence outcomes.
 - **Perpetual adaptivity**, which enables systems to modify their behavior or outputs in response to inputs, interactions, feedback, or changing conditions.
 - **Autonomy**, which enables systems to perform functions or make decisions with limited human intervention and oversight.
 - **Scalability**, where the ability to maintain or improve performance across larger volumes of data or tasks, may amplify existing biases and errors.
 - **Speed**, where the ability to process information, perform tasks or generate outputs within a short timeframe increases the scale and impact of benefits or errors, potentially outpacing effective human oversight.
9. [Appendix 1](#) maps select technologies against characteristics relevant to considering potential circumstances that create or amplify threats to compliance with the fundamental principles.

¹¹ The IAASB has identified and used certain of these characteristics in its work (without aiming to be comprehensive), and has recognized that various characteristics of emerging technologies may affect how quality risks are identified and addressed from a QM perspective.

The Five Fundamental Principles



Integrity



Objectivity



**Professional
Competence & Due
Care**



Confidentiality



**Professional
Behavior**

Technology Characteristic

- Opacity
- Non-deterministic
- Data dependence
- Perpetual adaptivity
- Autonomy
- Scalability
- Speed

Potential circumstances creating or amplifying threats

- Overreliance on technology and/or outputs
- Limited explainability
- Bias
- Reduced or limited human oversight
- Privacy and security risks
- Accountability gaps
- Amplified errors at scale
- Third-party reliance
- Lack of effective governance controls

Types of Threat

- Self-review
- Self-interest
- Intimidation
- Familiarity
- Advocacy

C. KEY ETHICAL CONSIDERATIONS

10. The Code applies to all PAs, whether in public practice¹² or business, regardless of the professional activities undertaken. Complying with the fundamental principles and specific requirements of the Code enables PAs to meet their responsibility to act in the public interest.¹³

Applying the Conceptual Framework

11. The conceptual framework¹⁴ sets out the approach to be taken by PAs to identify, evaluate and address threats to compliance with the fundamental principles and, for audits and other assurance engagements, threats to independence.
12. In applying the conceptual framework, PAs are required to have an inquiring mind, exercise professional judgment and use the reasonable and informed third party test¹⁵ when assessing whether the use of technology gives rise to threats to compliance with the fundamental principles, whether individually or in combination. This includes critically evaluating whether technology-driven outputs are reasonable and consistent with the facts and circumstances



known to the PA¹⁶ and determining whether their use is appropriate for the intended purposes.¹⁷

13. The ethical considerations apply throughout the entire lifecycle of technologies, including their design, procurement, implementation, operation, updating, replacement, and disposal. The role and responsibilities of the PA might vary depending on whether the PA

12 Consistent with paragraph 300.3 in Part 3 of the Code, references to a PA in this publication in the context of PAs in public practice include individual PAs in public practice and their firms.

13 Paragraph 100.6 A1

14 Section 120

15 Paragraph 120.5 A9: The reasonable and informed third party test is a consideration by the PA about whether the same conclusions would likely be reached by another party. Such consideration is made from the perspective of a reasonable and informed third party, who weighs all the relevant facts and circumstances that the accountant knows, or could reasonably be expected to know, at the time the conclusions are made. The reasonable and informed third party does not need to be an accountant, but would possess the relevant knowledge and experience to understand and evaluate the appropriateness of the accountant's conclusions in an impartial manner.

16 Paragraphs 120.5 A1 – A2

17 Paragraphs R220.8 and R320.11

is involved in developing or designing technology solutions, procuring third-party technologies, implementing technology within an organization, or relying on outputs generated by such technologies.¹⁸ Regardless of the extent of automation or whether the technology is internally developed or externally procured, the responsibility and accountability for professional judgments and decisions remain with the PA.

14. Technologies are often deployed in combination rather than in isolation, and their interaction may create or amplify ethical threats, which may not be the case when each technology is used alone. PAs should therefore consider not only the ethical implications of individual technologies, but also the cumulative and interconnected effects of integrated technology solutions. For example, AI and machine learning may be combined with data analytics, cloud computing, robotic process automation, or blockchain technologies within a single solution, resulting in increased complexity, opacity, and potential impacts on transparency, accountability, privacy, and decision-making. Accordingly, ethical evaluations should take a holistic approach¹⁹ that considers how multiple technologies interact across the broader technological ecosystem.²⁰

Characteristics of Emerging Technologies that May Create or Amplify Threats to the Fundamental Principles

15. Because of their characteristics, the use of emerging technologies may give rise to circumstances that create or amplify threats to compliance with the fundamental principles. Such circumstances include, for example, overreliance on technology (automation bias), limited explainability, reduced human oversight, privacy and data security vulnerabilities, accountability gaps, and the amplification of errors across systems and processes.
16. The **opacity** of some AI systems may make it difficult for a PA to understand how outputs are generated

or to explain the systems to clients, management, regulators, or other stakeholders. Such opacity may result in limited explainability, creating or amplifying a self-interest threat to compliance with the principles of integrity, objectivity, professional competence and due care, and professional behavior if decisions are made or communicated without a sufficient understanding of the basis for the output. Applying an inquiring mind and exercising professional judgment, the PA might question whether sufficient information is available to support reliance on the output,²¹ or whether there is a need to consult with an expert.²²

17. Technologies with **non-determinism** characteristics might produce differing results even when presented with identical or similar inputs. Placing undue reliance on such technologies creates or amplifies a self-interest threat to compliance with the principles of integrity, objectivity, professional competence and due care, and professional behavior if judgments or decisions are made based on the outputs without appropriate inquiry, monitoring or validation.
18. Technologies that exhibit **perpetual adaptivity** might evolve or modify their outputs over time based on new data, interactions, or changing conditions. Using such technologies could result in circumstances where users are unaware of, or do not sufficiently understand, how the system's behavior has changed. A PA might face greater adverse consequences from threats to integrity, objectivity, professional competence and due care, and professional behavior if outputs are accepted without appropriate monitoring, validation, or ongoing assessment of the system's performance and reliability.
19. In both circumstances where **non-determinism** and **perpetual adaptivity** are present, the PA should exercise professional judgment²³ in determining the nature and extent of inquiry, monitoring or validation needed, including the extent of human oversight. Having an inquiring mind assists a PA in identifying circumstances where outputs appear incomplete, biased, inconsistent with other available information, or affected by errors amplified at scale.

18 A relevant consideration when using the output of technology is whether the PA is in a position to obtain information in relation to the factors necessary to determine whether such use is appropriate (paragraphs 220.12 A4 and 320.12 A1).

19 Paragraphs R120.7 and 120.7 A1

20 Paragraph 120.8 A1

21 Paragraphs 120.5 A1, R220.8 and R320.11

22 Paragraphs 120.5 A5, 220.8 A1 and 320.11 A1

23 Paragraph R120.5

20. **Data dependency** and associated data quality, either on their own or in combination with other characteristics, may give rise to bias in AI models or to the generation and dissemination of inaccurate information across interconnected systems. Such cases create an advocacy threat where PAs promote or support analyses or positions that may be based on biased or misleading information. In addition, widespread or rapidly propagated errors in autonomous systems may increase the severity of threats to compliance with the fundamental principles because the consequences of failures can occur at scale and before effective human intervention is possible.
21. **Scale** and **speed** characteristics, while not only resulting from automation, are often related to **autonomy** and interconnected systems, and may result in amplified errors, like bias, misinformation, or unauthorized actions. For example, automated decision-making tools integrated across multiple systems may rapidly propagate inaccurate information, execute transactions without sufficient human oversight, or expose confidential information through cybersecurity or privacy weaknesses. These circumstances create or amplify threats to compliance with the fundamental principles. Reduced human oversight over significant judgments or decisions, or weaknesses in such oversight, may create a self-interest threat if PAs place undue reliance on automated outputs to improve efficiency or reduce costs, rather than exercising appropriate professional judgment. Possible actions that might address these threats include having an appropriate human oversight and review process, by clearly assigning accountability for decisions made or supported by automated systems, using experts where necessary to evaluate the reliability and limitations of systems, and segregating duties to reduce the risk of unauthorized or inappropriate actions. Such actions may eliminate the threats or reduce them to an acceptable level.
22. **Scalability** and **perpetual adaptivity** may give rise to circumstances that further amplify threats to compliance with the fundamental principles because the technologies can affect large volumes of information, transactions, or stakeholders simultaneously. In addition, frequent updates or changes to models underlying the technologies may alter system behavior in ways that are not immediately apparent. A PA should therefore assess threats on an ongoing basis, rather than treating the assessment as a one-time exercise.²⁴ An ongoing approach to threat assessment could include periodically reviewing the appropriateness and adequacy of safeguards, monitoring for unintended consequences, reassessing whether there continues to be a sufficient level of human oversight, and evaluating whether continued use of the technology remains appropriate for the intended purposes.
23. The Code sets an expectation that PAs remain alert to whether new information has emerged or changes in facts and circumstances have occurred that impact the level of a threat or affect the PA's conclusion regarding whether safeguards applied continue to be appropriate.²⁵ If so, the Code requires the PA to re-evaluate and address that threat accordingly.²⁶ For instance, a PA may initially determine that the use of a third-party software tool is appropriate, having evaluated the vendor's controls, data sources, and the reliability of the model's outputs, and having implemented safeguards such as periodic review and human oversight. However, over time, the model may be subject to model drift²⁷ or the vendor may update the software or modify its algorithms without full transparency. These developments constitute new information or changes in circumstances that could increase the risk of bias, errors, or lack of explainability, thereby elevating threats to compliance with the fundamental principles. In such cases, the Code requires the PA to reassess the situation, determine whether the existing safeguards remain effective, and implement additional measures if necessary to ensure that the PA continues to uphold the fundamental principles.
24. The circumstances in which PAs carry out professional activities and factors affecting the identification and evaluation of threats vary in range and complexity. PAs should be alert to the greater need to exercise

24 Paragraph R120.9 and 300.7 A7

25 Paragraph 120.9 A1

26 Paragraphs R120.9 and 300.7 A7

27 Where its performance degrades due to changes in underlying data patterns.

professional judgment,²⁸ drawing on their skills and training, and an understanding of the relevant facts and circumstances to determine appropriate courses of action.²⁹ This includes, for example, critically assessing technology-driven outputs,³⁰ understanding their limitations,³¹ and considering whether additional expertise or consultation is required.³² In this context, emerging technologies do not diminish the role of professional judgment; rather, they amplify its importance in ensuring that decisions are well-informed, objective and sound.

25. [Appendix 2](#) illustrates how certain characteristics of technologies may lead to circumstances that create or amplify threats to compliance with the fundamental principles.

Further Considerations for Emerging Technologies

26. Maintaining professional competence and due care³³ in an environment of rapidly evolving technologies requires an ongoing commitment to continuous learning and the development of appropriate technological literacy. The level of understanding required will depend on the nature of the technology and the PA's role in relation to it.³⁴ However, a PA is expected to have, or obtain, a sufficient understanding of the technology to evaluate whether its use is appropriate and whether reliance may be placed on its outputs.³⁵ The Code requires the PA to exercise professional judgment when the PA applies the conceptual framework in order to make informed decisions about the courses of action available and

determine whether such decisions are appropriate. In making such determination, the PA might consider the need to consult with others with relevant expertise or experience.³⁶

27. When implementing or using technologies, PAs are also encouraged to apply appropriate guardrails aligned with both leading technological practices and established controls.³⁷ For example, organizations may prohibit the use of "shadow information technology (IT)"³⁸ to mitigate risks associated with unapproved or unvetted software. Such use can increase risks associated with emerging technologies, including the misuse of AI and heightened exposure to cybersecurity vulnerabilities.
28. The wide availability of technologies such as AI also increases fraud risks due to the ability of criminal actors to use such technologies to create deepfakes,³⁹ synthetic data, or other highly convincing fabricated content. These technologies may be susceptible to manipulation, potentially undermining the reliability of outputs, representations, and other related information.
29. In addition, the regulatory environment for technologies continues to evolve rapidly across various jurisdictions. Accordingly, PAs should maintain an up-to-date understanding of applicable regulatory requirements⁴⁰ and ensure ongoing compliance with them as technologies and regulatory frameworks continue to develop.

28 Paragraph 120.5 A4 – A5

29 Paragraph 120.5 A6 – A8

30 Paragraphs 120.5 A1 – A2

31 Paragraph R113.3

32 Paragraphs 220.8 A1 and 320.11 A1

33 Paragraph R113.1

34 Paragraphs 113.1 A2 – A3, 220.12 A4 and 320.12 A1

35 Paragraphs R220.8 – 220.8 A1, R320.11 – 320.11 A1

36 Paragraph 120.5 A5

37 For firms that are subject to the IAASB's QM standards, the matter of guardrails may be addressed within their systems of quality management, which includes the fulfilment of responsibilities in accordance with relevant ethical requirements.

38 Shadow IT occurs when employees use IT resources independently of the organization's official IT infrastructure to meet specific business needs or improve productivity.

39 AI-generated synthetic media such as videos, images, or audio that are created or modified to convincingly imitate real people or events.

40 Paragraph R115.1. For example, laws and regulations relating to privacy, data protection, cybersecurity, anti-money laundering, consumer protection, intellectual property, or the use of digital assets and automated decision-making systems.



D. CONCLUSION

30. The IESBA will continue providing ethical guidance to assist PAs in addressing technology-related threats, while continuing its technology-focused work in the years ahead. The IESBA will also continue to coordinate with the IAASB regarding its technology-related activities to reinforce the connectivity and interoperability of the IESBA Code and the IAASB's QM and engagement standards.
31. As technology rapidly reshapes the global financial system and the accountancy profession, it is critical that these developments are addressed in a manner that enables PAs to fulfill their responsibility to act in the public interest and sustain confidence in the profession. This evolving landscape underscores the importance of adaptability, continuous learning,⁴¹ and a strong ethical foundation to ensure that technological advancement supports, rather than undermines, the integrity of, and public trust in, the profession.
32. Ultimately, regardless of the level of automation or technological sophistication, PAs remain responsible for the judgments and decisions made in their work.
33. The [IESBA Technology Focus](#) page provides a centralized source of information on IESBA's work related to technology, including publications, guidance materials, thought leadership, and updates on emerging technology developments and their implications for ethics and independence.

41 A PA is required to maintain professional competence by having a continuing awareness and understanding of technical, professional and technology-related developments relevant to the professional activities undertaken by the PA (paragraph 113.1 A3).

APPENDIX 1

Illustrative Mapping of Technologies Against Characteristics that May Give Rise to Circumstances that Create or Amplify Threats

The table below provides an illustrative and non-exhaustive mapping of select technologies against characteristics that may give rise to circumstances that create or amplify threats to compliance with the fundamental principles. The purpose of the table is not to suggest that the presence of a particular characteristic will necessarily give rise to circumstances that result in a threat. Rather, the table is intended to help PAs and other stakeholders identify characteristics that technologies exhibit which, depending on the facts and circumstances, may lead to or increase the significance, scale, speed, unpredictability, or complexity of ethical risks.

Not all implementations of a technology will exhibit these characteristics to the same extent, and emerging or evolving uses may alter the relevance or significance of particular characteristics over time.

PAs need to exercise professional judgment in interpreting the table and evaluating the ethical implications of specific technologies within their particular context.

Technology	Opacity	Non-determinism	Data dependence	Perpetual Adaptivity	Autonomy	Scalability	Speed
Agentic AI	✓	✓	✓	✓	✓	✓	✓
Distributed Ledger Technologies	–	–	✓	–	✓	✓	✓
Generative AI	✓	✓	✓	✓	✓	✓	✓
Machine Learning	✓	✓	✓	✓	✓	✓	✓
Quantum Computing	✓	✓	✓	–	–	✓	✓
Robotic Process Automation	–	–	✓	–	✓	✓	✓

APPENDIX 2

Characteristics of Technologies and Potential Circumstances that Create or Amplify Threats

Technology Characteristics	Potential circumstances creating or amplifying threats	Examples of Fundamental Principle impacted	Examples of threat ⁴²
Opacity	- Limited explainability of outputs and decisions - Inability to understand how conclusions were reached - Difficulty challenging or validating results - Overreliance on vendor assurances - Limited transparency into vendor controls	- Professional competence and due care - Integrity - Objectivity - Professional behavior	Intimidation Self-interest
Non-determinism	- Identical or similar input producing different outputs - Unpredictable responses - Inconsistent advice or conclusions - Difficulty reproducing evidence or audit trails	- Professional competence and due care - Integrity - Objectivity - Professional behavior	Intimidation Self-interest
Perpetual Adaptivity	- System behavior changes after deployment without explicit reprogramming - Controls becoming outdated - Risk assessments no longer valid - Evolving outputs reducing reliability	- Professional competence and due care - Integrity - Objectivity - Professional behavior	Intimidation Self-interest

⁴² For a description of types of threat, see paragraph 120.6 A3. For practical guidance in identifying threats, refer to [Exploring the IESBA Code Installment 2 of 12](#).

Technology Characteristics	Potential circumstances creating or amplifying threats	Examples of Fundamental Principle impacted	Examples of threat ⁴²
Autonomy	• Reduced human intervention or approval • Excessive delegation of judgment to systems • Diminished professional skepticism • Accountability gaps regarding decisions made by technology	• Professional competence and due care • Objectivity • Integrity • Confidentiality • Professional behavior	Self-interest Advocacy
Data dependence	• Biased, incomplete, inaccurate, or outdated data influencing outputs • Privacy breaches • Unauthorized data use • Embedded historical bias affecting recommendations	• Objectivity • Confidentiality • Integrity • Professional behavior	Self-interest Advocacy
Scalability	• Errors, bias, or inappropriate outputs replicated rapidly across large populations or transactions • Widespread impact before detection • Amplified compliance failures	• Professional competence and due care • Objectivity • Integrity • Professional behavior	Intimidation Self-interest
Speed of processing and decision making	• Reduced time for human review or challenge • Automation bias • Pressure to accept outputs without sufficient scrutiny • Insufficient due diligence	• Professional competence and due care • Objectivity • Integrity • Professional behavior	Intimidation Self-interest Advocacy

The *International Code of Ethics for Professional Accountants (including International Independence Standards)*, Exposure Drafts, Consultation Papers, and other IESBA publications are copyright of IFAC.

The International Foundation for Ethics and Audit™ (IFEATM), the International Ethics Standards Board for Accountants (IESBA®) and the International Federation of Accountants® (IFAC®) do not accept responsibility for loss caused to any person who acts or refrains from acting in reliance on the material in this publication, whether such loss is caused by negligence or otherwise.

Copyright © July 2026 by the International Federation of Accountants (IFAC). All rights reserved.

Written permission is required to translate, reproduce, store or transmit, or to make similar uses of this document, save for where the document is being used for individual, non-commercial use only. Permission to make copies of this document does not extend to the use of this publication for training or operating artificial intelligence systems without prior written permission from IFAC.

The 'International Ethics Standards Board for Accountants', 'International Code of Ethics for Professional Accountants (including International Independence Standards)', 'International Ethics Standards for Sustainability Assurance (including International Independence Standards)', 'Non-compliance with laws and regulations', 'International Federation of Accountants', 'IESBA', 'IFAC', 'IESSA', 'NOCLAR' and the IESBA logo are trademarks of IFAC, or registered trademarks and service marks of IFAC in the US and other countries. The 'International Foundation for Ethics and Audit' and 'IFEATM' are trademarks of IFEA, or registered trademarks and service marks of IFEA in the US and other countries.

For copyright, trademark, and permissions information, please visit [Permissions](#) or contact Permissions@ifac.org.



www.ethicsboard.org |  [@ethics_board](https://twitter.com/ethics_board) |  [company/iesba](https://www.linkedin.com/company/iesba)