

**Emerging Technologies:  
A Characteristic-based Approach to Ethical Considerations for Professional  
Accountants**

**Contents**

A.	Introduction .....	2
B.	Characteristics Associated with Emerging Technologies .....	3
C.	Key Ethical Considerations .....	4
D.	Conclusion .....	8
	Appendix 1.....	10
	Appendix 2.....	11

## A. Introduction

1. Technology continues to reshape how organizations operate, deliver value, and manage risk. 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 technologies<sup>1</sup> have long been used by professional accountants (PAs), emerging technologies<sup>2</sup> increasingly exhibit characteristics – for instance opacity, non-deterministic behavior, 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.
3. As emerging technologies evolve,<sup>3</sup> they introduce not only efficiencies and innovations, but also new challenges related to ethics, governance,<sup>4</sup> security, human oversight and accountability. The use of emerging technologies may give rise to circumstances or conditions that create or amplify threats<sup>5</sup> to compliance with the fundamental principles of the [\*International Code of Ethics for Professional Accountants \(including International Independence Standards\)\*](#) (the Code). These circumstances or conditions include, for example, automation bias and lack of explainability.
4. The IESBA's 2023 [\*Technology-related Revisions\*](#),<sup>6</sup> 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 common characteristics associated with emerging technologies may create or amplify threats to such compliance. By centering guidance on these characteristics rather than on specific

### The Technology-Related Revisions

- Strengthened the Code in guiding the mindset and behavior of PAs when they use technology.
- Introduced enhanced guidance 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.

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> These technologies move at different speeds along the maturity curve. Some remain experimental, while others are rapidly becoming embedded in core operations.

<sup>4</sup> 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.

<sup>5</sup> 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).

<sup>6</sup> [IESBA Technology Project](#)

technologies or situations, the publication is designed to support PAs across a wide range of technologies and contexts. The IESBA will complement this publication with subsequent technology-specific guidance.

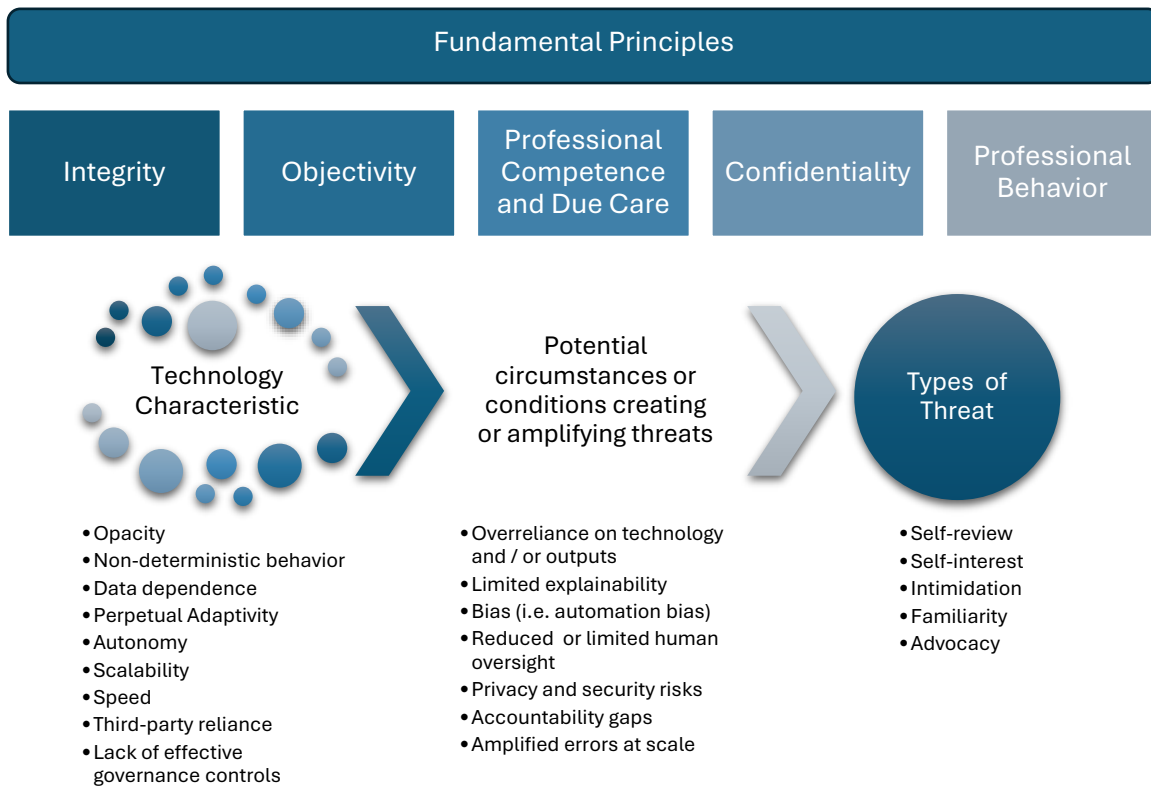
## B. Characteristics Associated with Emerging Technologies

6. In the last decade, significant advances in computing power have enabled technologies to be deployed at a 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.
7. Emerging technologies exhibit characteristics that, individually or in combination, can create or amplify threats to compliance with the fundamental principles.<sup>7</sup> These characteristics include:<sup>8</sup>
  - **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-deterministic behavior**, 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 and speed**, which amplifies both the benefits and risks associated with them.
  - **Dependence on third-party providers**, which may reduce control over system design, data and models used, operation, security, reliability or compliance, and may create additional risks relating to accountability, confidentiality, or resilience.
  - **Lack of effective governance controls**, because regulatory frameworks and governance structures are typically slow to develop and adapt.

---

<sup>7</sup> The five fundamental principles are integrity, objectivity, professional competence and due care, confidentiality, and professional behavior (paragraph 110.1 A1).

<sup>8</sup> This is not intended to be a complete list of characteristics that emerging technologies could exhibit. This list will be reviewed periodically by IESBA Staff to assess the need for any updates.



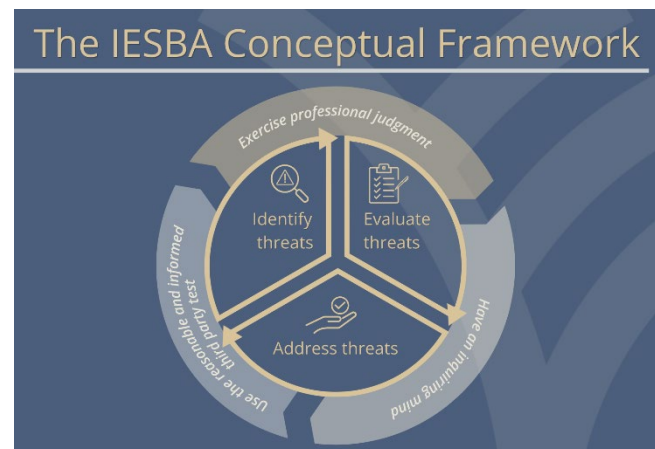
[Appendix 1](#) maps select technologies against characteristics that may create or amplify threats to compliance with the fundamental principles.

## C. Key Ethical Considerations

- The Code applies to all PAs, whether in public practice or business, regardless of the professional activities undertaken. Compliance with the fundamental principles and specific requirements of the Code enables PAs to meet their responsibility to act in the public interest.<sup>9</sup>

### Applying the Conceptual Framework

- The conceptual framework<sup>10</sup> sets out the approach to be taken to identify, evaluate and address threats to compliance with the fundamental principles and, for audits and other assurance engagements, threats to independence.
- In applying the conceptual framework, PAs are required to have an inquiring mind, exercise professional judgment and use



<sup>9</sup> Paragraph 100.6 A1

<sup>10</sup> Section 120

the reasonable and informed third party test<sup>11</sup> 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 PA<sup>12</sup> and determining whether their use is appropriate for the intended purposes.<sup>13</sup>

11. 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 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. 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.
12. 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 approach that considers how multiple technologies interact across the broader technological ecosystem.

### **Characteristics that May Create or Amplify Threats**

13. As mentioned, the nature and level of the threats might be influenced by the characteristics of the technologies (refer to [Section B](#)). These characteristics might give rise to circumstances or conditions that create or amplify threats to compliance with the fundamental principles. Such circumstances or conditions include, for example, overreliance on technology (automation bias), limited explainability, reduced human oversight, privacy and security vulnerabilities, accountability gaps, and the amplification of errors across systems and processes.
14. For instance, the opacity of some AI systems might make it difficult for a PA to understand how outputs are generated or to explain the systems to clients, management, regulators, or other stakeholders. Limited explainability could create 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 sufficient understanding of the basis for the output. Applying an inquiring mind and exercising professional judgment, the PA might question whether sufficient information is

---

<sup>11</sup> 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.

<sup>12</sup> Paragraphs 120.5 A1-A2

<sup>13</sup> Paragraphs R220.8 and R320.11

available to support reliance on the output,<sup>14</sup> whether alternative sources of evidence are needed, or whether additional expertise should be obtained.

15. Technologies with non-deterministic behavior might produce differing results even when presented with identical or similar inputs. This could increase the risk that users place undue reliance on technology-driven outputs without appropriate inquiry, monitoring, or validation. Technologies that exhibit adaptive behavior might evolve or modify their outputs over time based on new data, interactions, or changing conditions. This could create additional risks 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 objectivity if outputs are accepted without appropriate monitoring, validation, or ongoing assessment of the system's performance and reliability.
16. In both circumstances of non-deterministic and adaptive technologies, the PA should exercise professional judgment in determining the nature and extent of inquiry, monitoring or validation needed, including the extent of human oversight. Having an inquiring minds assist a PA in identifying circumstances where outputs appear incomplete, biased, inconsistent with other available information, or affected by amplified errors generated at scale.
17. Autonomous and highly interconnected systems can also increase the scale and speed at which errors, bias, misinformation, or unauthorized actions occur. For example, automated decision-making tools integrated across multiple systems might rapidly propagate inaccurate information, execute transactions without sufficient human oversight, or expose confidential information through cybersecurity or privacy weaknesses. These circumstances or conditions may create or amplify threats to compliance with the fundamental principles. For example, reduced human oversight over significant judgments or decisions 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.
18. Biases embedded in AI models or inaccurate information generated and disseminated across interconnected systems may create an advocacy threat where PAs inadvertently promote or support misleading information, analyses or positions. In addition, widespread or rapidly propagated errors in autonomous systems may increase the severity of such threats because the consequences of failures can occur at scale and before effective human intervention is possible. Examples of actions that might address threats include appropriate human oversight and review process, 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.
19. Scalability and perceptual adaptation may further amplify threats to compliance with the fundamental principles because technologies can affect large volumes of information, transactions, or stakeholders simultaneously. In addition, frequent updates or changes to models 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. An ongoing approach to threat assessment could include periodically reviewing the appropriateness and adequacy of

---

<sup>14</sup> Paragraphs R220.8 and R320.11

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.

20. 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.<sup>15</sup> If so, the Code requires the PA to re-evaluate and address that threat accordingly.<sup>16</sup>
21. 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 drift<sup>17</sup> 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.
22. The circumstances in which PAs carry out professional activities and factors involved vary in range and complexity. PAs should be alert to the greater need to exercise professional judgment,<sup>18</sup> drawing on their skills and training, and an understanding of the relevant facts and circumstances to determine appropriate courses of action.<sup>19</sup> This includes, for example, critically assessing technology-driven outputs,<sup>20</sup> understanding their limitations,<sup>21</sup> and considering whether additional expertise or consultation is required.<sup>22</sup> 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.
23. [Appendix 2](#) illustrates how certain characteristics of technologies may lead to circumstances or conditions that create or amplify threats to compliance with the fundamental principles.

### Key Considerations Not Unique to Emerging Technologies

24. Maintaining professional competence and due care<sup>23</sup> 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

---

<sup>15</sup> Paragraph 120.9 A1

<sup>16</sup> Paragraphs R120.9 and 300.7 A7

<sup>17</sup> Where its performance degrades due to changes in underlying data patterns

<sup>18</sup> Paragraph 120.5 A4 – A5

<sup>19</sup> Paragraph 120.5 A6 – A8

<sup>20</sup> Paragraphs 120.5 A1-A2

<sup>21</sup> Paragraph R113.3

<sup>22</sup> Paragraphs 220.8 A1 and 320.11 A1

<sup>23</sup> Paragraph 113.1 A2

the technology and the PA's role in relation to it. 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.<sup>24</sup> The Code requires the PA to exercise professional judgement when the PA applies the conceptual framework in order to make informed decisions about the courses of actions 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.<sup>25</sup>

25. The implementation of technologies should include appropriate guardrails aligned with both leading technological practices and established controls. For example, organizations may prohibit the use of "shadow information technology (IT)"<sup>26</sup> to mitigate risks associated with unapproved or unvetted software. Such practices can increase risks associated with emerging technologies, including the misuse of AI and heightened exposure to cybersecurity vulnerabilities.
26. 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,<sup>27</sup> 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.
27. 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 requirements<sup>28</sup> and ensure ongoing compliance with them as technologies and regulatory frameworks continue to develop.

## **D. Conclusion**

28. The IESBA will continue to play a key role in providing ethical guidance to assist PAs in addressing technology-related risks, while continuing its technology-focused work in the years ahead.
29. As technology rapidly reshapes the 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 sustains confidence in the profession. This evolving landscape underscores the importance of adaptability, continuous learning,<sup>29</sup> and a strong ethical foundation to ensure that technological advancement supports, rather than undermines, the integrity of, and public trust in, the profession.

---

<sup>24</sup> Paragraph R113.1

<sup>25</sup> Paragraph 120.5 A5

<sup>26</sup> Shadow IT occurs when employees use IT resources independently of the organization's official IT infrastructure to meet specific business needs or improve productivity.

<sup>27</sup> AI-generated synthetic media such as videos, images, or audio that are created or modified to convincingly imitate real people or events.

<sup>28</sup> 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.

<sup>29</sup> 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)



30. Ultimately, regardless of the level of automation or technological sophistication, PAs remain responsible for the judgments and decisions made in their work.

### **Helpful links and resources**

#### *Technology*

- [Applying the Code's Conceptual Framework to Independence: Practical Guidance for Auditors in Technology-related Scenarios](#)
- [IESBA Technology Working Group's Phase 2 Report](#)
- [Ethical Leadership in a Digital Era: Applying the IESBA Code to Selected Technology-Related Scenarios](#)
- [Exploring the IESBA Code: A Focus on Technology](#)
- [Exploring the IESBA Code: A Focus on Technology - Artificial Intelligence](#)
- [Mindset and enabling skills of professional accountants: Paper 4 \(CPA Canada, ICAS, IFAC, IESBA\)](#)
- [Identifying Mitigating Bias and Mis- and Dis-information: Paper 3 \(CPA Canada, ICAS, IFAC, IESBA\)](#)
- [Technology is a double-edged sword with opportunities and challenges for the accountancy profession: Paper 2 \(CPA Canada, ICAS, IFAC, IESBA\)](#)
- [Ethical Leadership in an Era of Complexity and Digital Change: Paper 1 \(CPA Canada, ICAS, IFAC, IESBA\)](#)
- [Ethical Leadership in an Era of Complexity and Digital Change: Exploratory Paper \(CPA Canada, ICAS, IFAC, IESBA\)](#)

#### *Other*

- [IESBA Staff Questions & Answers - Using the Work of an External Expert](#)

## Appendix 1

### Illustrative Mapping of Technologies Against Characteristics that May Create or Amplify Threats

The table below provides an illustrative and non-exhaustive mapping of select technologies against characteristics that may 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 necessarily results 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 should therefore exercise professional judgment in interpreting the table and evaluating the ethical implications of specific technologies within their particular context.

Technology	Opacity	Non-deterministic behavior	Data dependence	Perpetual Adaptivity	Autonomy	Scalability	Speed	Third-party reliance	Lack of effective governance controls
Agentic AI	✓	✓	✓	✓	✓	✓	✓	✓	✓
AI Orchestration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Distributed Ledger Technologies	–	–	✓	–	✓	✓	✓	✓	✓
Data Analytics	✓	–	✓	✓	–	✓	✓	✓	✓
Generative AI	✓	✓	✓	✓	✓	✓	✓	✓	✓
Machine Learning	✓	✓	✓	✓	✓	✓	✓	✓	✓
Quantum Computing	✓	✓	✓	–	–	✓	✓	✓	✓
Robotic Process Automation	–	–	✓	–	✓	✓	✓	✓	✓

## Appendix 2

### Characteristics of Technologies and Potential Circumstances or Conditions that May Create or Amplify Threats

Technology Characteristics	Potential circumstances or conditions creating or amplifying threats	Examples of Fundamental Principle impacted	Examples of threat
Opacity	<ul style="list-style-type: none"> <li>Limited explainability of outputs and decisions</li> <li>Inability to understand how conclusions were reached</li> <li>Difficulty challenging or validating results</li> <li>Overreliance on vendor assurances</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Integrity</li> <li>➤ Objectivity</li> <li>➤ Professional behavior</li> </ul>	Self-interest
Non-deterministic	<ul style="list-style-type: none"> <li>Identical or similar input producing different outputs</li> <li>Unpredictable responses</li> <li>Inconsistent advice or conclusions</li> <li>Difficulty reproducing evidence or audit trails</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Integrity</li> <li>➤ Professional behavior</li> </ul>	Self-interest
Perpetual Adaptivity	<ul style="list-style-type: none"> <li>System behavior changes after deployment without explicit reprogramming</li> <li>Controls becoming outdated</li> <li>Risk assessments no longer valid</li> <li>Evolving outputs reducing reliability</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Objectivity</li> <li>➤ Professional behavior</li> </ul>	Self-interest
Autonomy	<ul style="list-style-type: none"> <li>Reduced human intervention or approval</li> <li>Excessive delegation of judgment to systems</li> <li>Diminished professional skepticism</li> <li>Accountability gaps regarding decisions made by technology</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Objectivity</li> <li>➤ Integrity</li> <li>➤ Confidentiality</li> <li>➤ Professional behavior</li> </ul>	Self-interest Self-interest Advocacy
Data dependence	<ul style="list-style-type: none"> <li>Biased, incomplete, inaccurate, or outdated data influencing outputs</li> <li>Privacy breaches</li> <li>Unauthorized data use</li> <li>Embedded historical bias affecting recommendations</li> </ul>	<ul style="list-style-type: none"> <li>➤ Objectivity</li> <li>➤ Confidentiality</li> <li>➤ Integrity</li> <li>➤ Professional behavior</li> </ul>	Self-interest
Scalability	<ul style="list-style-type: none"> <li>Errors, bias, or inappropriate outputs replicated rapidly across large populations or transactions</li> <li>Widespread impact before detection</li> <li>Amplified compliance failures</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Integrity</li> <li>➤ Professional behavior</li> </ul>	Self-interest

<b>Technology Characteristics</b>	<b>Potential circumstances or conditions creating or amplifying threats</b>	<b>Examples of Fundamental Principle impacted</b>	<b>Examples of threat</b>
Speed of processing and decision making	<ul style="list-style-type: none"> <li>• Reduced time for human review or challenge</li> <li>• Automation bias</li> <li>• Pressure to accept outputs without sufficient scrutiny</li> <li>• Insufficient due diligence</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Objectivity</li> <li>➤ Integrity</li> <li>➤ Professional behavior</li> </ul>	Intimidation Self-interest
Third-party reliance	<ul style="list-style-type: none"> <li>• Unclear accountability for errors or misconduct</li> <li>• Limited transparency into vendor controls</li> <li>• Contractual and jurisdictional risks</li> </ul>	<ul style="list-style-type: none"> <li>➤ Professional competence and due care</li> <li>➤ Professional behavior</li> <li>➤ Confidentiality</li> <li>➤ Integrity</li> </ul>	Self-interest