



Toolkit: How to approach ethical challenges

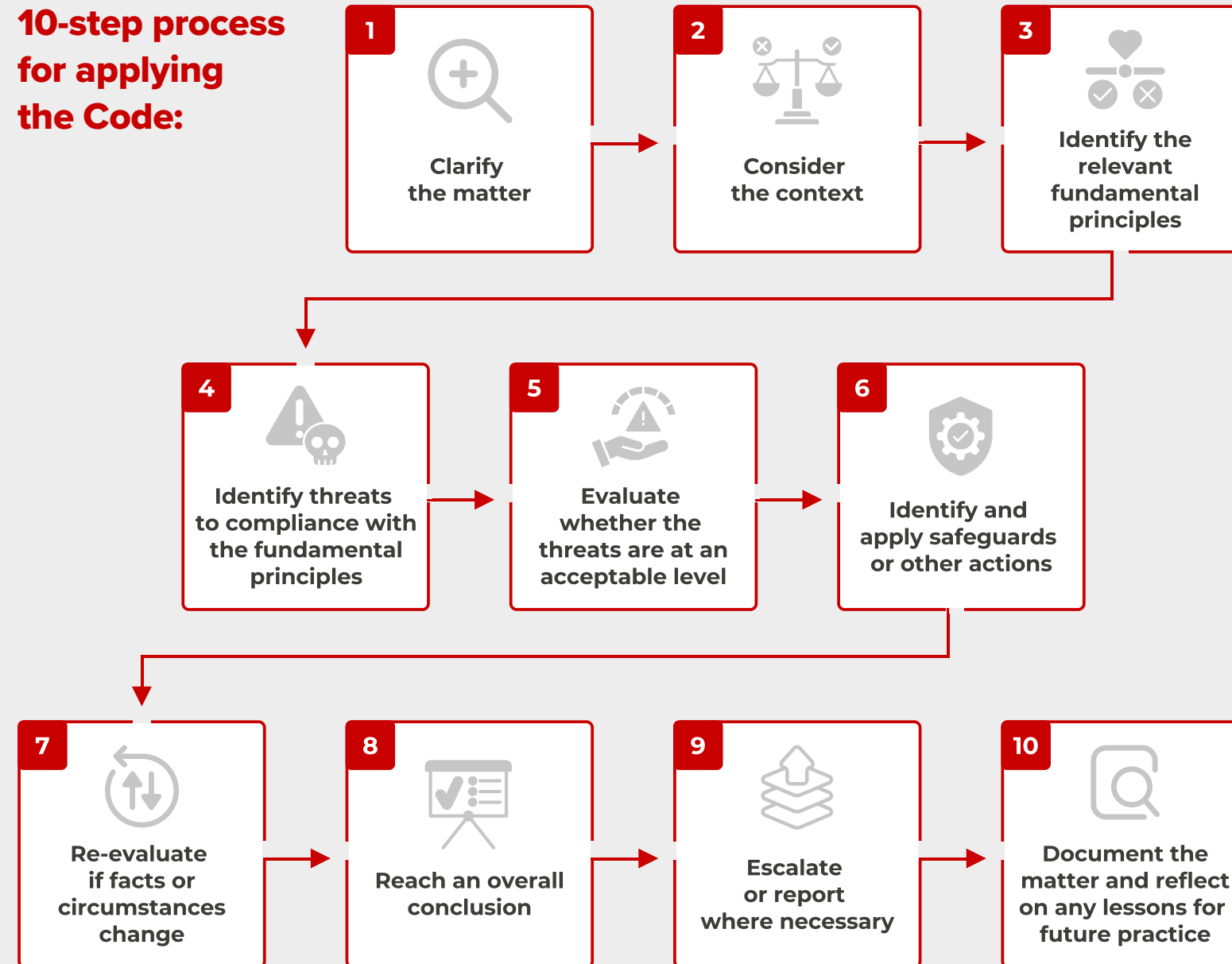
The purpose of this Toolkit is to provide a practical 10-step process for applying the Code in real situations.

It should be read as a guide to applying the conceptual framework and supporting ethical judgement in practice – not as a substitute for the specific provisions that apply to the role or engagement concerned.

ACCA adopts the [IESBA Code](#) in full as its Code of Ethics and Conduct. Professional accountants are required to comply with the fundamental principles and apply the conceptual framework to identify, evaluate and address threats to compliance with the fundamental principles. Applying the conceptual framework requires having an inquiring mind, exercising professional judgement, and using the reasonable and informed third-party test.

The fundamental principles remain the ethical anchor of the accountancy profession, as set out in Part 1 of the Code: integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour. Additional requirements and application material relevant to the application of the conceptual framework are set out in Part 2 of the Code for professional accountants in business, Part 3 for professional accountants in public practice, the International Independence Standards in Parts 4A and 4B, and Part 5 for sustainability assurance, as applicable.

10-step process for applying the Code:



1. Clarify the matter

Start by clearly identifying the matter that has arisen, or might arise. Define the decision, transaction, communication, report, instruction, or course of action that is causing concern. Separate established facts from assumptions, incomplete information, or untested impressions.



2. Consider the context

Consider the context in which the issue has arisen, or might arise. This includes the organisational environment, applicable laws and regulations, relevant professional standards, governance arrangements, stakeholder pressures, and the nature and purpose of the work being performed. Where relevant:

- This should include whether the matter relates to financial information, non-financial information, sustainability information, or the use of the work of others – and whether the surrounding facts increase the risk of bias, pressure, or inappropriate reliance.
- Consider whether the matter involves the use of AI or other technology – and whether that use affects the quality of evidence, the reliability or explainability of outputs, the risk of bias, confidentiality, the exercise of professional judgement, or the extent of reliance being placed on the work.
- Consider not only the use of a single tool – but the combined effect of connected technologies, data sources, automation features, and human workflow dependencies.

Where an ethical challenge, concern or judgement involves AI use, see our [practical prompt checklist for AI use](#) to support reflection, further review, and documentation.



3. Identify the relevant fundamental principles

Consider which of the five fundamental principles may be affected: integrity, objectivity, professional competence and due care, confidentiality, or professional behaviour.

Questions at this stage may include:

- Could the action involve information that is false, misleading, incomplete, or biased?
- Could ethical judgement be compromised by self-interest, familiarity, undue influence, incentives, or pressure?
- Do I have the necessary competence, capabilities, time, and support to carry out this work properly?
- Am I placing undue reliance on data, systems, experts, or the work of others without sufficient evaluation?
- Does the situation raise concerns about conduct that could breach laws or regulations, or discredit the profession?

Where AI is involved, the key ethical challenge is not simply that technology has been used, but whether its use affects compliance with the fundamental principles.

AI use may affect integrity if for example:

- outputs are false, misleading, incomplete, or insufficiently supported
- objectivity if automation bias, convenience, pressure, or over-reliance weakens independent judgement
- professional competence and due care if the output is not properly understood, tested or verified
- confidentiality of sensitive information is used or exposed inappropriately
- professional behaviour concerns if the use of AI creates legal, regulatory or reputational challenges.

In all cases, human accountability remains with the professional accountant for the final advice, decision or output. Our [practical prompt checklist for AI use](#) may be used as a supporting prompt where AI use forms part of the ethical challenge.



4. Identify threats to compliance with the fundamental principles

Apply the conceptual framework by identifying threats to compliance with the fundamental principles. These threats may fall into one or more of the following categories:

- self-interest
- self-review
- advocacy
- familiarity
- intimidation.

A single set of facts may create multiple threats, and may affect more than one fundamental principle. In practice, ethical threats often arise through recurring challenge areas such as AI use, organisational pressure, conflicts of interest, reporting integrity, and wider external demands.

We've created a [practical prompt checklist](#) to help identify threat indicators and consider whether further review, safeguards, consultation, escalation, or documentation is needed.



5. Evaluate whether the threats are at an acceptable level

Evaluate whether identified threats are at an acceptable level. This requires ethical judgement informed by the facts and circumstances known at the time – while remaining consistent with the Code's requirement to exercise professional judgement in applying the conceptual framework.

In making this assessment, consider the source, relevance and sufficiency of the information available – and whether preconception or bias might be affecting the exercise of ethical judgement.



6. Identify and apply safeguards or other actions

If threats are not at an acceptable level, they must be addressed. They can be addressed through safeguards – actions, individually or in combination, that effectively reduce threats to an acceptable level. Depending on the circumstances, actions might include:

- obtaining further information or evidence
- consulting others with relevant expertise
- using an appropriate reviewer
- strengthening supervision or oversight
- separating responsibilities
- communicating with management or those charged with governance.



7. Re-evaluate if facts or circumstances change

If new information emerges – or if facts and circumstances change – re-evaluate the threats and address them accordingly. This is particularly important where technology, stakeholder expectations, organisational pressures, or the scope of work changes over time.



8. Reach an overall conclusion

Before proceeding, reach an overall conclusion about whether the threats have been eliminated or reduced to an acceptable level – and whether the proposed course of action complies with the fundamental principles. This conclusion should reflect ethical judgement in practice, while remaining consistent with the Code's requirement to apply the conceptual framework with an inquiring mind and professional judgement.



9. Escalate or report where necessary

If the matter cannot be resolved at the working level, consider whether it should be escalated internally to the appropriate level of management or to those charged with governance. Consultation may be relevant where complying with one fundamental principle conflicts with one or more of the other fundamental principles.

Where pressure is being exerted, do not allow it to result in a breach of compliance with the fundamental principles. Where the matter involves non-compliance with laws and regulations, follow the applicable legal, regulatory and professional requirements.



10. Document the matter and reflect on any lessons for future practice

Document the facts considered, the ethical judgement exercised, consultations undertaken, and actions taken where appropriate. The Code encourages documentation of the substance of the issue, details of discussions, decisions made, and the rationale for those decisions.

After the matter is resolved, consider whether it reveals a wider issue in systems, governance, capability, incentives, or culture that should be addressed in future practice.

Where AI use forms part of the matter, documentation should include the:

- nature of the AI tool's use
- extent of reliance placed on it
- checks performed
- ethical judgement exercised
- reasons why the final decision or output was considered appropriate.

Our [practical prompt checklist for AI use](#) may assist in structuring that work where AI use forms part of the matter.