

# EXPLORING THE IESBA CODE

## Installment 4: The Conceptual Framework – Step 3, Addressing Threats



The IESBA Code helps professional accountants (PAs) meet their responsibility to act in the public interest. The Code provides a conceptual framework which specifies a three-step approach that all PAs are to apply in order to identify, evaluate and address threats to compliance with the Code’s fundamental principles.

The first Installment of Exploring the IESBA Code explained the Code’s five fundamental principles. Installment 2 highlighted three steps specified in the conceptual framework and examined how PAs are to identify threats to compliance with the principles. Installment 3 focused on evaluating threats, including how to use the reasonable and informed third party test to determine whether a threat is at an acceptable level. The next step is to address threats that are not at an acceptable level.



If any identified threats are determined to not be at an acceptable level, then the PA must take steps to address them by:

- Eliminating the circumstance, interest or relationship creating the threat(s);
- Applying safeguards (where available) to reduce the threat(s) to an acceptable level; or
- Declining or ending the specific professional activity or engagement that gives rise to the threat(s).

**PAs have an ongoing obligation to remain alert for changes in facts and circumstances that might impact the evaluation of the level of threats and the appropriateness of safeguards. If such changes arise, the PA must re-evaluate and address that threat.**

**Addressing Threats:** Let’s revisit the evaluation of the level of threats from Installment 3. What actions could the Director of Accounting Policy who works for an international manufacturing company take to address the threats that are not at an acceptable level?

The CEO has outlined a plan to set up operations in an emerging market. As Director of Accounting Policy, you are not sure the plan complies with bribery and corruption laws.

The company recently lost market share in a strategically important country and the stock has lost 10% of its market value as a result. A credible new plan for entering a high-margin market will satisfy the Board of Directors and shareholders. The CEO has promised sizable bonuses if the team can “get the job done, whatever it takes.”

You have reviewed email communications—several of which suggest that money has been transferred to external bank accounts in the target country while the new business plan was being developed.

**The Director has carefully applied the conceptual framework and, in doing so, systematically considered each category of threat using the reasonable and informed third-party test to determine that the following three threats are not at an acceptable level.**

Threats to professional behavior, integrity, objectivity, and professional competence and due care.

**Self-Interest**—The promise of large bonuses could make the Director hesitant to investigate the emails uncovered, less objective in evaluating the situation, or less diligent in understanding anti-bribery laws.

**Familiarity**—The Director might be “too close” to the situation and inclined to agree with the CEO’s plan out of implicit trust in the CEO and company decision-making.

**Intimidation**—The CEO’s “whatever it takes” approach could pressure the Director to just find the “right” answer.



**Safeguards are actions, individually or in combination, that the professional accountant takes to effectively reduce threats to compliance with the fundamental principles to an acceptable level.**

**Possible Actions to Address Threats**

These threats could be eliminated by cancelling the expansion plan (not in the Director’s control) or by ending the professional activity by resigning (possibly premature at this stage).

Alternatively, the Director could consider potential safeguards to reduce the threats such that a reasonable and informed third party would feel that the Director is acting in a manner that is consistent with the Code’s five fundamental principles.

- 1. Suggest to the CEO that the Board should be consulted/involved:** Involving the Board brings independent oversight to the decision-making process and helps ensure that due care and objectivity are brought to bear in evaluating and managing risks.
- 2. Consult with external legal counsel or advisors with expertise in the jurisdiction:** Engaging experts—not part of the CEOs team—introduces an effective impediment to moving ahead without thoroughly considering all the facts and evidence (including the emails) for compliance with appropriate laws.

Involving one of these parties provides an outside perspective that adds objectivity, transparency, and oversight to help ensure that decision-makers will be more compelled to act objectively and demonstrate professional behavior, integrity, professional competence and due care. The Director may deem it appropriate to use one or more of these, or other, safeguards.

**WHERE TO GET ASSISTANCE?**



The conceptual framework is set out in Part 1, Section **120** of the Code. Additional provisions that are relevant to applying this framework are set out in Parts 2, 3, 4A and 4B, Sections **200**, **300**, **400** and **900** respectively.



The eCode, which is available at [www.IESBAeCode.org](http://www.IESBAeCode.org), is an on-line resource for accountants and other users of the Code. It provides quick and efficient access to the Code, making it easier to use, implement, and enforce.