Procurement Fraud and Abuse Risk Examination
BY SHERYL STECKLER AND TOM CAULFIELD

Five major steps an organization can take to safeguard against procurement fraud and abuse which are sufficient to prevent, detect, ensure prompt reporting, and/or the capability to respond to such threats—and—that management and the workforce understand their responsibilities to ensure procurement integrity.

The procurement function of any organization has the primary objective of obtaining goods and services of satisfactory quality and expected quantity at an honest and reasonable cost.

Other objectives of this function include:
- Providing fair, open, and equitable treatment to those interested in doing business with the organization;
- Helping drive the mission of the organization; and
- Acting in good faith within its procurements.

In sum, the objectives of the procurement function of any organization revolve around one central theme: *procurement integrity*.

Undeniably, the most significant threats to achieving or maintaining procurement integrity come from the 44 traditional procurement fraud and abuse schemes[1] and the myriad of ways each of those schemes can be performed[2]. In nearly all cases, these schemes are perpetrated within a shroud of deception by one or more individuals with a deep familiarity of the procurement processes. The success of these malicious acts are driven by the perpetrator's (or perpetrators'):

- Motivations;
- Ability to influence a decision point within a procurement phase; and
- Knowledge of the effectiveness of the organization's procurement integrity controls[3].

In short, the effectiveness of protection against fraud and abuse threats come from the strength of the organization's procurement integrity controls. Therefore, the question every procurement professional needs to ask is "are our procurement integrity controls winning the battle?"

In order to build the most effective procurement integrity controls, the organization must identify and understand its unique degree of risks from the traditional schemes of procurement fraud and abuse, along with management determining its risk tolerance. Establishing the organization's risk tolerance[4] involves:

- Knowing which schemes are most likely to occur;
- Knowing where vulnerabilities are present in the organization's procurement methods; and
- Knowing what the operational and financial impacts of each scheme would be should they occur.

This is all done with an organization-specific "Procurement Fraud and Abuse Risk Examination." With the knowledge gained from this focused and tailored risk examination, the organization is better positioned to design sound, effective, and cost-reasonable procurement integrity controls consistent with its overall business environment and risk tolerance.

Because there can be various approaches to identifying risks, it's important to briefly describe some of the key differences. An enterprise-wide risk assessment is normally focused on identifying risks associated with achieving organization-wide goals, maximizing performance, and identifying future risks, which include reductions in budgets and personnel or shifts in the market. Most of these assessments are performed to protect the organization's networks, investments, proprietary information, employees, and assets. Some organization perform an enterprise-wide "fraud" risk assessment targeting "financial statement fraud," "asset misappropriation," and "corruption." As this type of risk assessment is designed specifically to identify the organization overall fraud risk, the broad scope presents a challenge in revealing the specific vulnerabilities and costly risks associated within the procurement process.

---

1 *Abuse* is a contracting action that falls short of being criminal and a prudent procurement professional would not consider ethical or a necessary business practice given the same facts and circumstances. A *scheme* is the specific methodology used to commit, conceal, and benefit from the act.

2 For more information, see the "The Five Faces of Procurement Fraud, Abuse, and Noncompliance," and "Schemes of the Fraudster: Beat Them at Their Own Game," at www.Procurement-Integrity.net.

3 *Procurement integrity controls* are the processes, procedures, and management systems that are designed to provide reasonable assurance regarding the prevention, detection, prompt reporting, and response capability to procurement fraud and abuse.

4 *Risk tolerance* is the level of risk that an organization is prepared to accept in pursuit of its objectives, and before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of an action (e.g., accelerated procurements with less segregation of duties) and the threats of fraud that might occur.

Without a specific assessment of the fraud schemes, the people that deploy them, how they are performed in the organization's specific procurement processes, and (most important) the effectiveness of the procurement prevention and detection mitigation controls, the organization will not fully appreciate its unique degree of vulnerability. Therefore, it will be unable to comprehensively safeguard against two of the largest-impact risks: "Financial" and "Reputation."

Five Major Steps to a Procurement Fraud and Abuse Risk Examination[5]

1. **Management's Perceived Vulnerabilities**
   Interview to identify the following:
   - Management's perception of areas within procurement and operations that are vulnerable to certain fraud and abuse schemes;
   - The potential financial, operational, and reputational impacts of a successful fraud or abuse scheme; and
   - The degree of potential noncompliance with internal procurement policies, procedures, and/or processes designed to prevent and detect fraud and abuse (i.e., procurement integrity controls).

2. **Documented Guidelines Vulnerabilities**
   Using existing organizational documents:
   - Perform an analysis of the procurement integrity controls' effectiveness against the traditional procurement fraud and abuse schemes and the people that commit those schemes; and
   - Develop "procurement scheme risk theories" on how a particular portion of the procurement process could be compromised focusing on the following elements:
     - The specific schemes that could compromise this process;
     - At which specific decision point (occupation) would these specific schemes appear; and
     - The specific steps required for the schemes to occur.

3. **Employee Perceived Vulnerabilities**
   With the aid of interviews:
   - Identify the workforce's perception of vulnerability of the traditional schemes;
   - Obtain their understanding on the effectiveness of the procurement integrity controls;
   - Gage their belief of likelihood of occurrence of the traditional schemes;
   - Gather information on the operational and financial impact of the more likely schemes; and
   - Determine any differences between management and the workforce in perceptions of vulnerabilities, risk tolerance, and commitment to procurement integrity.

4. **Testing Vulnerabilities**
   With each of the more likely schemes identified:
   - Interview the employees linked to that particular procurement process and obtain the interviewees' perceptions on the probability of occurrence and compromise; and
   - Interview other employees involved with the organization's procurement integrity controls (e.g., the audit department or the enterprise risk manager).

5. **Summarize Results**
   Starting with those schemes that present the greatest threats of occurrence:
   - Perform an analysis to identify the contributing factors, which can include, among other things:
     - Nonexistent or ineffective procurement policy,
     - Lack of workforce training on compliance with particular mitigation controls, and/or
     - Inadequate communication of risk tolerance thresholds;
   - Develop appropriate corrective actions to reduce the future probability of occurrence for those schemes identified; and
   - Continue with the more likely schemes based on degree of vulnerability, continuously making corrective actions consistent with management's risk tolerance thresholds.
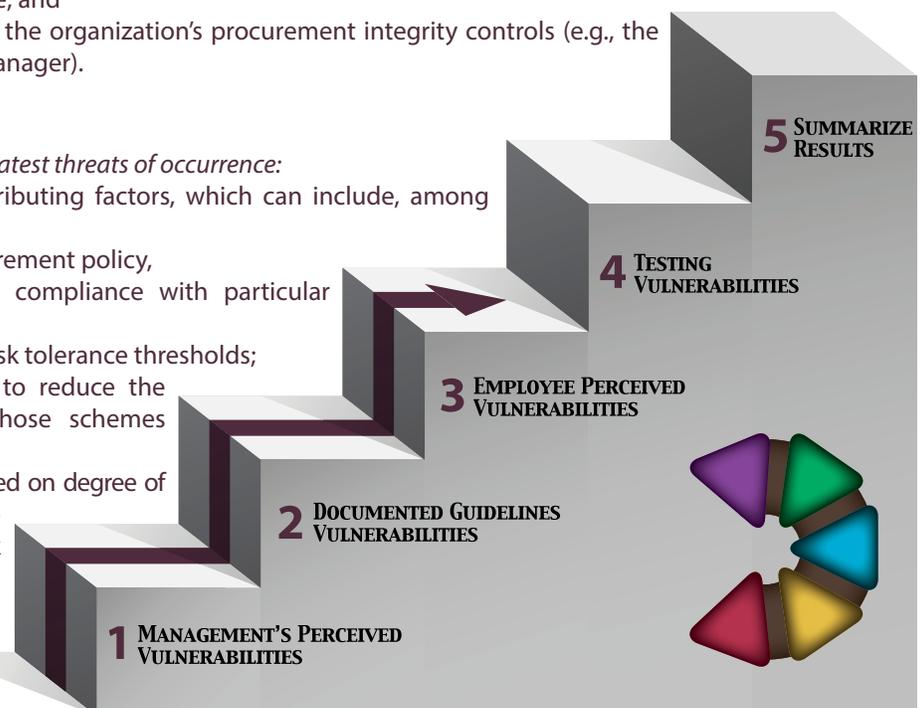
5   *Please note that it is beyond the scope of this article to describe in detail each step of a Procurement Fraud and Abuse Risk Examination. Therefore, overarching descriptions of the five major steps have been provided.*

Closing

An organization that wishes to ensure procurement integrity in order to safeguard against unnecessary financial losses and reputational damages related to today's malicious schemes of procurement fraud and abuse must:

- Identify its unique degree of risks to the traditional schemes of procurement fraud and abuse,
- Evaluate the effectiveness of its procurement integrity controls against those same schemes,
- Measure its commitment to procurement integrity, and
- Establish risk thresholds.

This can only be done effectively with a Procurement Fraud and Abuse Risk Examination. Because much of this type of assessment involves anticipating the behavior of a potential perpetrator, the assessment team must collectively have specialized backgrounds in the prevention and detection of procurement fraud and abuse—including experience in assessing mitigation controls, fraud risk, procurements, and organizational culture.

Now, picture the organization you work for. Imagine if management and the workforce were asked the following questions:

- What are the four most likely fraud and abuse threats to your organization's procurements?
- What are four prevention and detection mitigation controls that are currently in place to protect your organization's procurements?
- What is expected of you to ensure procurement integrity?

Could they answer? Could you? It's your duty to ensure that your organization is best protected with sound procurement fraud and abuse prevention and detection mitigation controls.