CREATING A FRAUD RISK ASSESSMENT AND IMPLEMENTING A CONTINUOUS MONITORING PROGRAM

Compliance professionals around the world are struggling with how to do more with less. In order to provide effective assurance services that make your audit committee, executive management, and other stakeholders happy, it’s critical to identify and implement a risk-based approach to auditing. In this session, you will learn what makes a risk assessment robust and how to develop a continuous monitoring approach that achieves maximum results using audit software.

You will learn how to:

- Develop a robust risk assessment program.
- Perform a fraud risk assessment and come up with practical fraud scenarios.
- Create a continuous monitoring approach that detects red flags for investigation and follow-up.

CHRISTOPHER DILORENZO, CFE, CPA, CIA, CRMA, CISA
Vice President
Internal Audit
Scientific Games
Las Vegas, NV

Christopher M. DiLorenzo is currently the Vice President and Chief Audit Executive (CAE) for Scientific Games Corporation (SG) based in their Las Vegas corporate headquarters. SG recently acquired Bally Technologies where DiLorenzo had been a member of the internal audit function for the prior 11 years and CAE for the last five years. Prior to working for Bally Technologies, he worked in the internal audit department of the Mandalay Resort Group and was also in public accounting with both Andersen and Deloitte. Currently he is responsible for executing SG’s global internal audit program, which includes areas such as testing for Sarbanes-Oxley compliance, operational audits, and aiding in forensic investigations.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
Topics for Today
This presentation will cover four specific areas:

- Robust risk assessments
  - More specifically, what makes your assessment robust
- Understanding fraud
  - In order to create your assessment effectively, you need to get inside the mindset of the fraudster, understand what frauds are relevant to your company, and anticipate how the fraudster may try to perpetrate the scenario.
- Creating your fraud risk assessment
- Examples of how we developed a continuous monitoring approach to fraud

Robust Risk Assessments
In order to make your risk assessment, consider these four components:

- Make your assessments comprehensive.
  - Fraud is just one of the many components of a risk assessment that should be considered. Risk assessments should also consider: minimum requirements, such as compliance requirements; enterprise and strategic risk; operational and process risk; and, of course, fraud risk.
  - While creating this assessment, make sure that you’re working towards evaluating as many fraud risks as you’re able to identify. Using the ACFE fraud tree is a great resource.
- Make your assessments detailed.
  - For each risk event that you identify, make sure to capture all of the relevant attributes.
    - Why does the risk need to be mitigated?
      * It is important to document complete risk event statements; this will be critical when devising your testing and/or continuous monitoring plan.
* Always add the “…” to each risk statement. For example, don’t stop at “improper segregation of duties exist for cash disbursements”—make sure to finish the risk statement so we know “why” we’re concerned. Adding “… which may lead to lapping schemes, theft of cash/checks, inaccurate payments, etc.” will allow the auditor to develop audit plans.

**How risky is it?**
- Since we all have finite resources, risk events need to be measurable so we can appropriately allocate our time to provide the best assurance services possible. Make sure that your rating approach covers areas such as: How impactful is it if this risk were to occur? How likely is it to occur?

**What can we do about it?**
- Once you’ve identified what the risks are and how likely they are, your assessment should also point to where you are covering the risk (if at all).

**Where does it need to be addressed?**
- If your company has various operations/locations, it’s important to consider these risks in each applicable location. Your plan should define in which locations you see risk and in which location you recommend coverage.

**Who can address it?**
- At times, you may find that a risk needs audit coverage, but you don’t have the quantity/qualified resources to perform a monitoring function. Here you should identify “who” can/will address the risk.
  - When is the timing within our plan?
- Make sure your assessments are empowered. Your empowerment comes from areas such as:
  - Internal audit charter, audit committee
  - Board approval
  - Management buy-in/involvement
Understanding Fraud
In order to aid your company at preventing/detecting fraud, you must have a sound appreciation of fraud and how the mind of the fraudster works. The fraud triangle is a great starting point. A good mnemonic to use to remember the components of the triangle is that fraud can make a company “POR.” POR stands for pressure, opportunity and rationalization. As you begin defining your fraud risk events, understanding “who” may be the fraudster will help you hone in on the particular circumstances that you’re looking to monitor/mitigate. It will also help you identify potential control weaknesses.

Consider some of these key facts while planning your assessment:
- An estimated 5 percent of revenues are lost due to fraud each year.
- Median loss per incident was $145,000.
  - 22 percent of the cases were at least $1M.
- Median fraud duration lasted 18 months before detection.
- The presence of anti-fraud controls is associated with decreases in cost and duration of the scheme.
- COSO 2013 (Principle 8) requires that:
  - The organization considers the potential for fraud in assessing risks to the achievement of objectives.
- According to the 2014 ACFE Report to the Nations, more than 72 percent of the frauds were detected as a result of:
  - Tips (42.2%)
  - Management review (16%)
  - Internal audit (14.1%)
- 2014 ACFE Report to the Nations provided that, in nearly one-third of the cases reported, the victim organization lacked the appropriate internal controls to prevent the fraud.
Additionally, one-fifth of the reported cases could have been prevented if managers had done a sufficient job reviewing transactions, accounts or processes.

Creating Your Fraud Risk Assessment

While creating your fraud risk assessment, define a fraud universe. This can be aligned with other initiatives, such as SOX, by starting to consider fraud risk in each of your identified SOX processes and/or considering each key operational business area. Once you’ve built/organized your list of processes where the organization may be susceptible to fraud, begin to brainstorm applicable fraud scenarios. A great option to help in this process is the fraud tree—by using this tree and brainstorming applicable fraud risks from each area (if applicable), you’ll have a great starting point of risk events for your assessment and ultimate plan.

For each fraud risk event you define, make sure to include:

- Who the fraudster is
- The result of the fraud (or the “…”)
- How the fraudster benefits from committing the fraud (e.g., the conversion)
- The company’s internal control environment that will prevent or detect this event
  - If unknown, investigation is needed.
- Documentation of how the control function will work given the scenario
- Whether internal control gaps exist
- Provide this to business leaders over each process area and solicit their input—update accordingly
- Repeat this exercise for each business entity/location.

Next, we need to determine a level of risk for each of these events. Our approach is to use residual risk (versus inherent risk), which we define as the risk of an event happening
given the known control environment. We use two rating parameters for fraud: *likelihood of occurrence and impact of the event*, presuming that it took approximately thirty-six months to be detected. Our rating scale is:

**Immaterial**  
For this rating, we look solely at the impact rating. If the impact was a “1”, we consider the risk immaterial for the current assessment and reassess it in subsequent assessments.

**SOX Testing**  
As a publicly traded company required to comply with the Sarbanes-Oxley Act, we naturally have certain monitoring functions taking place. As a result, many controls exist in our environment that we will be testing irrespective of this assessment and with no additional impact. If a fraud risk is being mitigated by one of these SOX controls already identified for testing, we can link them together with no additional testing being required.

**Operational Review**  
If we haven’t removed the risk as a result of it being immaterial or linked it to already-planned SOX testing procedures, an operational review or other auditing procedures must be considered to provide sufficient coverage in your plan. That said, as resources may be an issue, your plan needs to consider the frequency for conducting these additional reviews. When we do our planning, we use a three-year audit cycle, which tends to provide us with adequate coverage and allows us to focus on these additionally identified areas in concert with any resource constraints that arise.
**Partial SOX/Partial Operational**
This classification is a combination of the SOX testing and operational review classifications. We use this one when SOX testing by itself provides some coverage, but not full coverage. For example, the existing SOX control/test may only cover one attribute, whereas the fraud risk event covers multiple attributes.

Lastly, we review each fraud risk event to determine if continuous monitoring procedures could be automated to provide regular assurance over the identified scenario.

**Creating a Continuous Monitoring Approach**
Continuing from the previous step, now that we have a list of areas where we may be able to develop a continuous monitoring approach, we need to continue the brainstorming process of how to systematically monitor.

**Planning and Brainstorming**
Create a theoretical approach for monitoring, and start meeting with the business to ensure appropriate access to the data, understand the corresponding data tables, and validate the workflow of transactions to ensure accurate knowledge of the process. Once this planning step is complete, use a dashboard slide to vet the plan as a group.

**Designing Your Continuous Monitoring Script**
After obtaining access to and understanding the data, it’s time to start creating the data logic that you will use to create your script. The data logic needs to be designed to help identify potential irregularities, which may take several iterations of your logic. The number of potential red flags or exceptions that result needs to be a manageable number in order to allow a reasonable
amount of follow-up time. Documentation of this process is also key in order to ensure that the data script and logic is documented in such a way that it can be easily understood and re-performed if necessary.

**Development**
As this section could be a course in itself, at a high level, it’s important to make sure that you have the proper tools to do the job, both within the expertise of your team and with a software tool such as ACL, IDEA, etc. While you’re documenting these scripts, you should always be concerned with the continuity of your continuous monitoring program, so your team must do a comprehensive job of documenting all steps in the development of the script. One of the worst things that could happen here is that you create a great program for monitoring only to lose it if you lose people on your team.

**Testing Your Analytics**
After you’ve designed your analytics and run the program, you likely have generated a list of false positives. This is expected and needs to be vetted. In some analytics, false positives will always arise, but a key to making your process efficient is to define your script to vet out as many false positives as you can, while not making your script miss actual red flag events. Vetting your exceptions is ideally done by the auditors obtaining supporting documentation, understanding that documentation, and performing light inquiries as necessary. Of course, depending on what you’ve found, proceed with caution on your inquiries because it is possible that you (a) came across a problem and don’t want to alert the fraudster early in your process, or (b) that management thinks that you’re
investigating them, which could create a contentious environment.

**Reviewing Your Output**

Reviews should take place both over the specifics of your script and those that you will be handing the script off to—e.g., business auditors (in our case). The goal of this phase is to ensure that documentation is sufficient, and that the scripts are working properly and meeting the objectives for why they were created.

**Deployment Phase**

Now that all other steps are completed, you’re ready to deploy your script and start the continuous monitoring function. At this stage, you should also:

- Identify how often monitoring should be performed, (e.g., daily, monthly, quarterly, etc.).
- Ensure that personnel are properly trained on the execution of the continuous monitoring program and the follow-up procedures.
- Have a plan for communicating test results within the department as well as to relevant upper management, as deemed necessary.
- Have consistent communication regarding unique findings or analytic improvements with your script developers. This is vital to keeping the continuous monitoring program current, efficient, and effective.