Best Practices for Auditing & Monitoring Your Ethics & Compliance Program

Jeffrey Kaplan
Kaplan & Walker LLP

John Peltier
The Network

WELCOME!

Please standby. Our webcast will begin shortly.

THE Network
Integrated GRC Solutions

Speaker Introduction

Jeff Kaplan is a partner in **Kaplan & Walker LLP**, a law firm in Princeton, New Jersey and Santa Monica, California.

For more than 20 years he has specialized in all aspects of assisting companies in developing, implementing and reviewing corporate compliance/ethics programs , and has also reviewed programs for several governmental agencies and the World Bank. He was for many years Counsel to the Ethics Officer Association (now the ECOA).

Jeff co-chairs the annual PLI annual Advanced C&E Workshop, is the Featured Risk Assessment Columnist for the Corporate Compliance Insights web site, and is editor of the Conflict of Interest Blog. He is formerly an Adjunct Professor of Business Ethics at the Stern School of Business, New York University.

Jeff is a member of the New York and New Jersey bars.

Jeff received his B.A. from Carleton College and his J.D. from Harvard University.

THE Network
Integrated GRC Solutions

Speaker Introduction

John Peltier leads The Network's product management team, responsible for the strategy and delivery of the integrated governance, risk and compliance software suite.

John previously led those efforts on our Policy Management and Learning Management Systems, and also spent time on our Product Marketing team.

John is an accomplished product management professional, with over a decade of experience delivering solutions to business problems. He has been in ethics and compliance since joining The Network in 2011, and previously spent nine years in healthcare.

THE Network
Integrated GRC Solutions

C&E: "Checking" Auditing, Monitoring and Assessments

Jeff Kaplan/Kaplan & Walker LLP
jkaplan@kaplanwalker.com
The Network; January 20, 2015

Today's Presentation

- **Auditing**
- **Monitoring**
  - But not all the uses of technology
- **Through two different lenses**
  - General program
  - Different risk areas (e.g., anti-corruption)
- **Assessments: risk, program and culture**
- **Relevance of "behavioral ethics" to checking**

General Observations

- **Official Expectations**
  - Auditing and monitoring have always been particularly important to the government
    - 1992 Antitrust Division statement
    - The 2010 compliance "half measures" FCPA case
- **As programs mature, promoting understanding (through policies and training) should become relatively less of a focus and ensuring actual compliance (through auditing and monitoring) become more of one**

General Observations

- **Auditing & monitoring are particularly important for:**
  - Global/highly dispersed companies
  - Those in highly regulated industries
  - Companies with cultural challenges

General Observations (cont.)

- **Relationships between relevant C&E categories can be confusing:**
  - **Auditing** can overlap with **program assessment**, and with risk assessment
  - The line between **auditing** and **investigations** is not always well marked
  - **Monitoring** can overlap with **governance** and management
  - **Metrics** are part of **monitoring**, but are sometimes discussed separately

General Observations (cont.)

- **Encouraging reports of suspected violations** can be seen as a form of **monitoring** – but is generally treated as a different animal
- **Other types** of internal controls (e.g., preapprovals) can also be viewed as a form of **monitoring** – but really serve a different function

Does this matter?

It can – If people are talking past each other.

General Observations (cont.)

- **The big picture is important – but so is the small one:**
  - Companies generally should be moving in the direction of "**nano compliance**"
    - Location or risk area specific
    - Learning to paint with a narrow brush
  - **Monitoring** in particular is a useful vehicle for this

Monitoring Generally

- **Monitoring differs from auditing in that it is:**
  - Less independent
  - More real time
- **Generally, an under-utilized C&E function**
- **Covers a lot of ground, but a major distinction is between monitoring by**
  - **Business people** – both risk area and general program
  - **Non-audit staff**

Monitoring By Business People

- **Monitoring is often called "the first line of defense"**
- **It is the most immediate – and least independent – form of C&E checking**
- **Risk-area examples include tasking managers to:**
  - T&E reviews by direct supervisors
  - Review of invoices of third parties for any indicia of corruption (or violation of other rules)
  - Review pricing and other activities for any indicia of antitrust violations
  - Monitoring COIs that have been conditionally okayed

Monitoring By Business People

- **Challenges to risk area monitoring**
  - Is it informed?
  - Is it documented?
  - Is it actually happening?
- **Note that this type of monitoring is often part of larger business monitoring**
  - E.g., of high-risk agents (making sure not only that they are acting properly but that they are doing what you want/pay them to do)

Monitoring By Business People (cont.)

- **General program monitoring**
  - Ensuring that employees in the manager's BU have taken required training
  - Seeing how lower level managers communicate about C&E to their subordinates
- Other points about **monitoring**
  - Serves to educate business people (learn by doing)
  - Provides a predicate for:
    - C&E-based compensation
    - "Supervisory liability" (meaning internal, not actual legal, accountability)

Monitoring By Business People

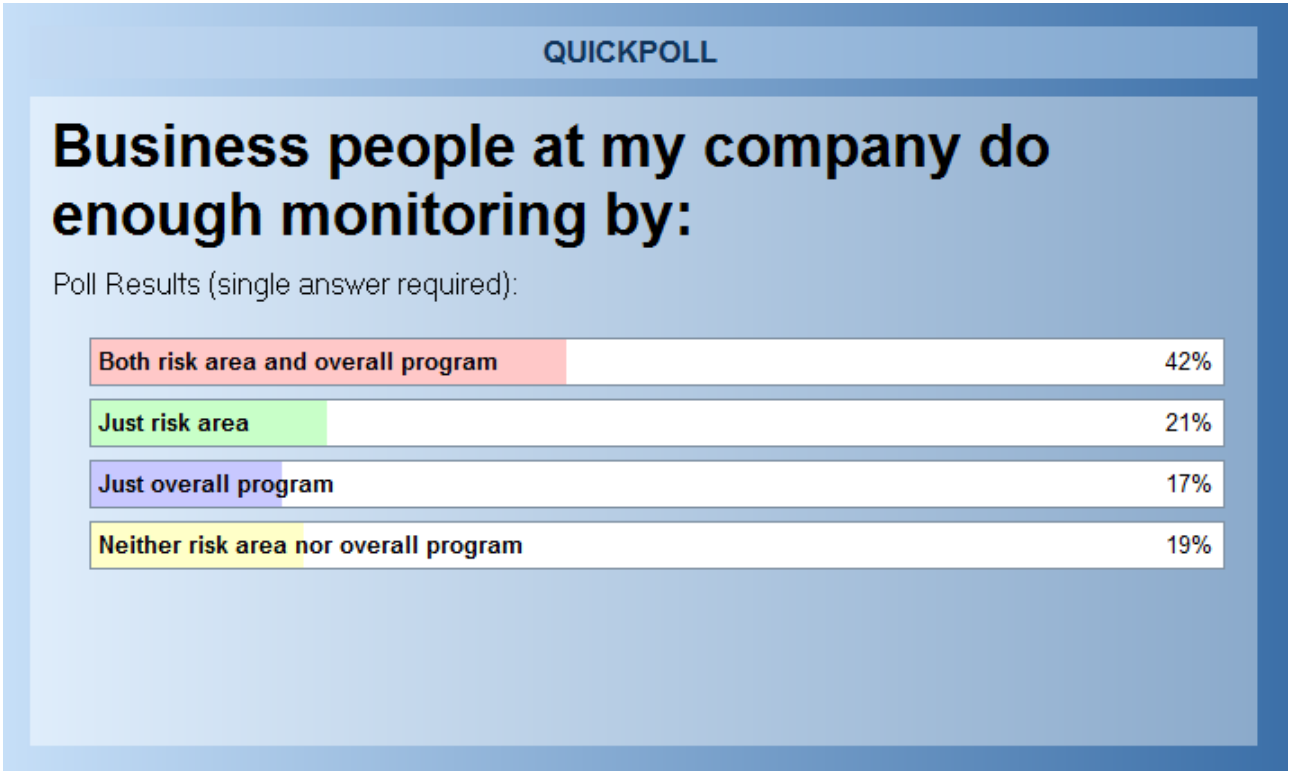
POLL QUESTION #1

Business people at my company do enough monitoring by…

- Both risk area and overall program
- Just risk area
- Just overall program
- Neither risk area nor overall program

Monitoring By Business People

POLL RESULTS #1



Monitoring By (Non-Audit) Staff

- **Non-Audit Staff**, includes:
  - Finance
  - Legal
  - HR
  - IS
  - EH&S
  - Security
  - C&E
- They are seen as non-independent because they may be reviewing their own work
- This is "**the second line of defense**"

Risk-Area Monitoring By Staff

- **Anti-corruption**
  - Periodic controls reviews by Finance
  - C&E reviewing gift registers and third party due diligence files
- **Competition Law**:
  - Legal department reviewing sales files
- **Employment:**
  - Looking for required postings
  - Reviewing personnel files
- **EH&S**: Many examples
- **Risk-Area Specific**
  - Life sciences "ride-alongs"
  - Review of trading at financial service firms

General Program Monitoring By Staff

- **Looking at:**
  - Training and communications
  - C&E concerns reporting
  - Investigations and discipline
  - Hiring and incentives
  - Mostly by the C&E office, but not exclusively
- **2 other forms of checking that are monitoring-like**
  - C&E questions in employee engagement survey
  - C&E questions in exit interviews

Monitoring By Staff

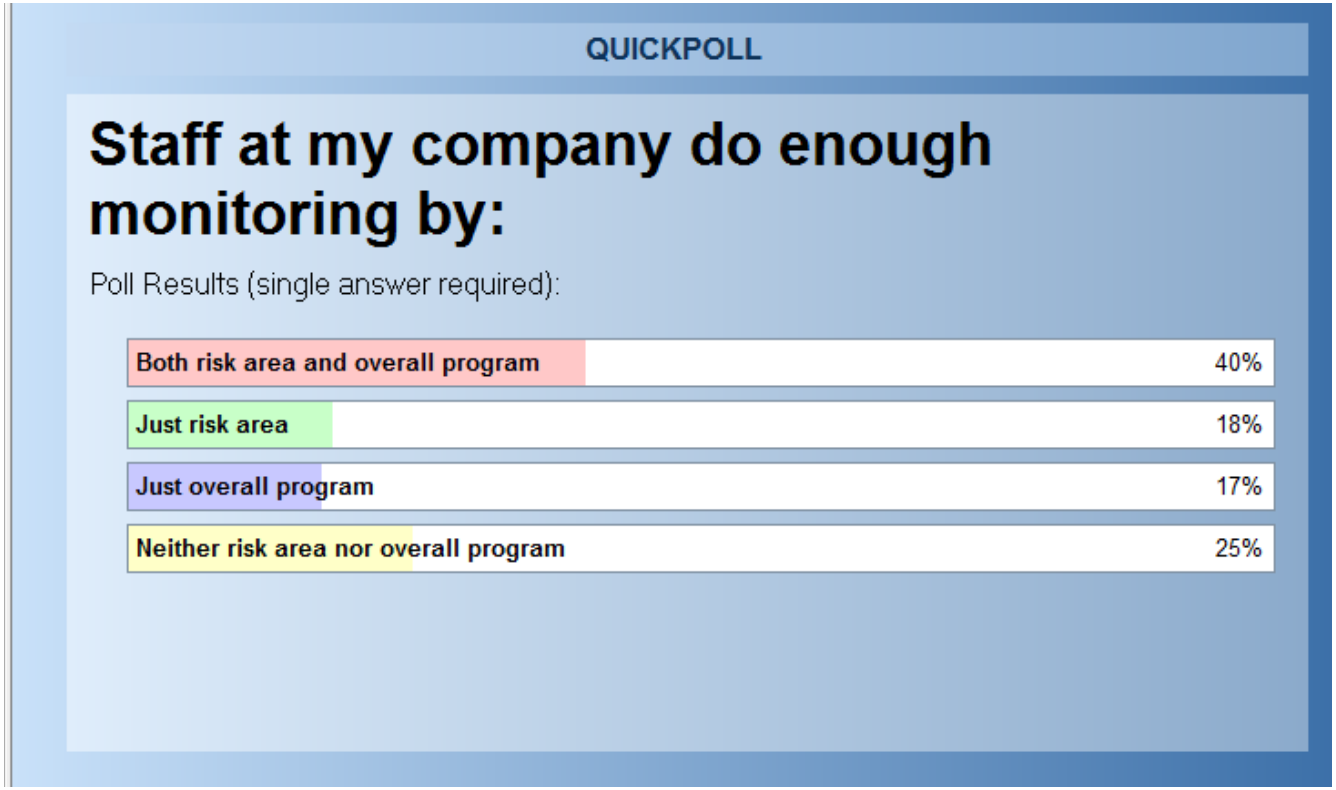
POLL QUESTION #2

Staff at my company do enough monitoring by:

- Both risk area and overall program
- Just risk area
- Just overall program
- Neither risk area nor overall program

Monitoring By Staff

POLL RESULTS #2



Monitoring – Where To Start?

- **A self-check tool (consider adding a geographic and/or product/service line to the tool)**
  - It would include both business personnel and staff monitoring
  - A note on "nature of the risk"

Area of law	Nature of risk	Current monitoring	Monitoring to consider adding
FCPA			
Antitrust			
etc.			

Auditing – General Points

- The "third line of defense"
- More independent and less frequent than monitoring
- Includes both internal and external
- C&E audits are
  - Sometimes stand-alone
  - More often part of broader audits
- Does having C&E part of audit planning process pose an independence problem?

Auditing (cont.)

- **Risk areas commonly audited**
  - FCPA
  - Fraud
  - Privacy
  - IP/confidential information
  - Trade controls
  - Industry-specific regulated areas
- **Many others**
- **Sometimes stand-alone, more often as part of more general audits**

Auditing (cont.)

- **General Program**
  - C&E reporting and investigations
    - Flows from *Caremark/Stone v Ritter*
  - Employee knowledge of program requirements
  - Auditing against governance requirements
    - E.g., regional committees
    - A good reason to have charters

Other Aspects of Auditing

- **Ensuring sufficient domain knowledge by auditors**
- **Ensuring follow up**
- **Should audit results be a metric?**
  - The Danger: Creating incentives to game the system
- **Can Audit serve in other C&E roles?**
  - Depends on how much
    - These roles involve exercise of judgment
    - You want to audit the roles
  - Training, investigations generally okay – designing controls a closer call

Compliance Auditing

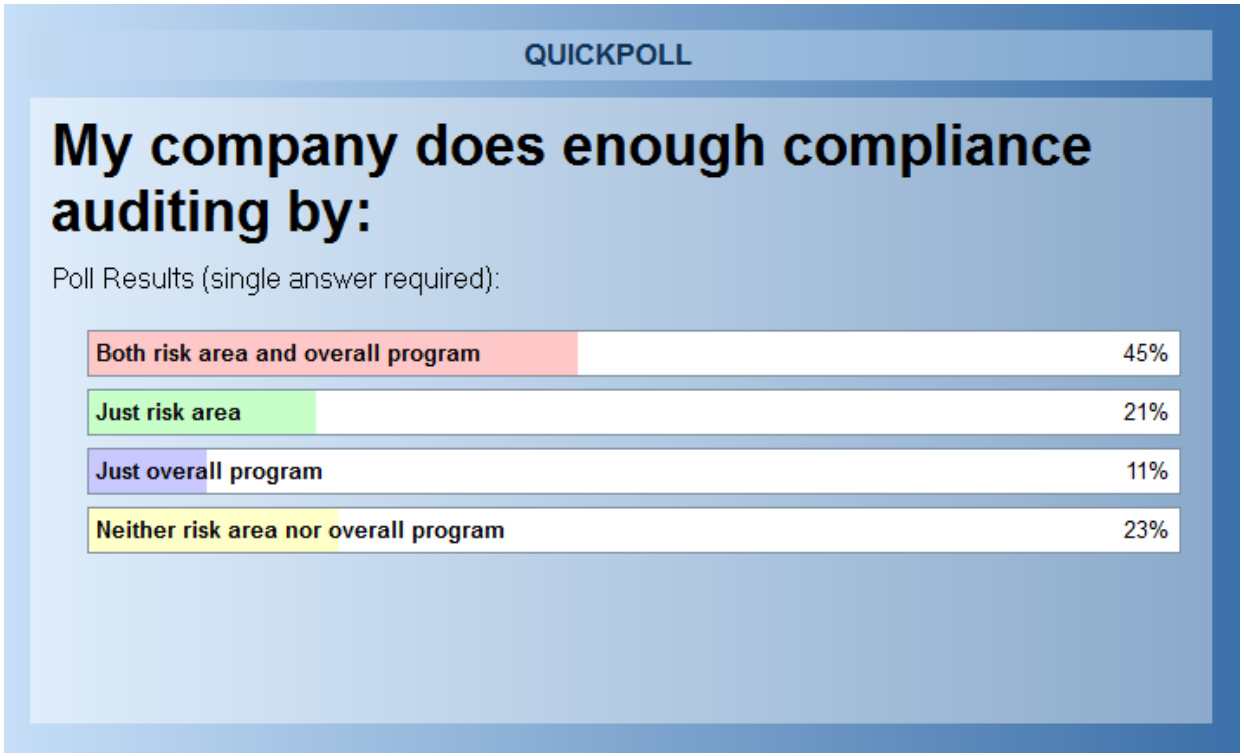
POLL QUESTION #3

My company does enough compliance auditing by:

- Both risk area and overall program
- Just risk area
- Just overall program
- Neither risk area nor overall program

Compliance Auditing

POLL RESULTS #3



Risk, Program & Culture Assessments

- **Assessments are generally more qualitative than audits**
- **There are many variations of Assessments**
- **6 general types:**
  - Actual assessments typically are a blend of more than one of these – rarely are they stand-alone
  - Hopefully this will help you do a needs assessment for your program, risk and culture assessments

Risk Assessment – Type 1

- **Risk areas that are the primary responsibility of the C&E office and that are both broad (meaning they touch many employees) and deep (meaning they have a potentially high impact)**
  - – e.g., corruption, competition law and possibly fraud
  - Be mindful of particular expectations for anti-corruption risk assessments
  - Don't neglect competition law
    - New official expectations from Italian government

Risk Assessment – Type 2

- **Risk areas that are the primary responsibility of the C&E office but are not so broad and/or deep**
  - In some companies, conflicts of interest (often broad, but not that deep) or insider trading (deep, but not typically that broad) fit into this category
  - Part of the assessment regarding confidential information will depend partly on how important such information is to a company)
  - You should generally cover these in assessments – but not necessarily to the same degree as type 1 risks

Risk Assessment – Type 3

- **Risk areas that may be broad and deep, but that are the primary responsibility of another function at the company**
  - In some companies, trade compliance or employment law would fit this bill
  - One might have a narrower gauge of inquiry in the interviews/document reviews, at least if such functions have already conducted some form of targeted assessment(s) regarding these risks
  - A good area for awareness questions

Program Assessment – Type 1

- **Program assessment: tools/elements about which many employees typically have information/views**
  - Examples include **C&E training** and the **helpline**
- **Most assessments include this, but how much to focus on it depends on various factors**
  - E.g., getting a wide array of feedback on training will make sense if you are considering overhauling your training
  - **Helpline/investigation assessments** particularly important for public companies due to *Caremark*

Program Assessment – Type 2

- **Tools/elements that relatively few employees have information/views about**
- **Examples include:**
  - Monitoring approaches
  - Pre-hiring due diligence
  - Board oversight
- **Need to cover, but often in different ways than type 1 assessment topics**

Culture Assessments

- **Relevant to both program and risk assessment**
  - But for planning purposes generally should be viewed as its own effort): factors that could impact both the degree of risk and the efficacy of the program
  - Examples include tone at the top, accountability, openness of communication and alignment of rewards with stated C&E values
  - Not just organizational cultures – but geographic and industry ones too
- **How deep should you dive?**
  - Depends on contemplated use of assessment
  - Boards of directors tend to care particularly about these sorts of assessments – because culture is where they can help

Finally, A Word About "Behavioral Ethics"

- Knowledge/ideas from behavioral economics applied to ethics

Overriding Lesson:
We are not as ethical as we think

- Can help to explain results of checking in ways that promote greater C&E efforts generally

For more lessons on risk assessments and other C&E functions see www.conflictofinterestblog.com under Interests – Bias tab

Questions?

Q&A

THE Network
Integrated GRC Solutions

Contact Us

Jeff Kaplan
Kaplan & Walker
Info@KaplanWalker.com
www.kaplanwalker.com
(609) 375-2350 (NJ Office)

THANK YOU!

John Peltier
The Network
JohnPeltier@tnwinc.com
www.tnwinc.com
(800) 253-0453

THE Network
Integrated GRC Solutions

Upcoming Events…

DOWNLOAD THE ON-DEMAND WEBCAST AND SLIDE DECK HERE:

https://www.tnwinc.com/10103/webinar-best-practices-auditing-monitoring-compliance-program/

THE Network
Integrated GRC Solutions