



FORENSIC

# Compliance Risk Management

## How to Deliver and Implement a Compliance Risk Assessment

ADVISORY

# Agenda

1. Why perform a formal compliance risk assessment ?
2. How to develop organizational support and sponsorship ?
3. How to conduct a compliance risk assessment ?
4. Reporting the results: leadership and the Board
5. Corrective action planning and implementation

# Chapter 1

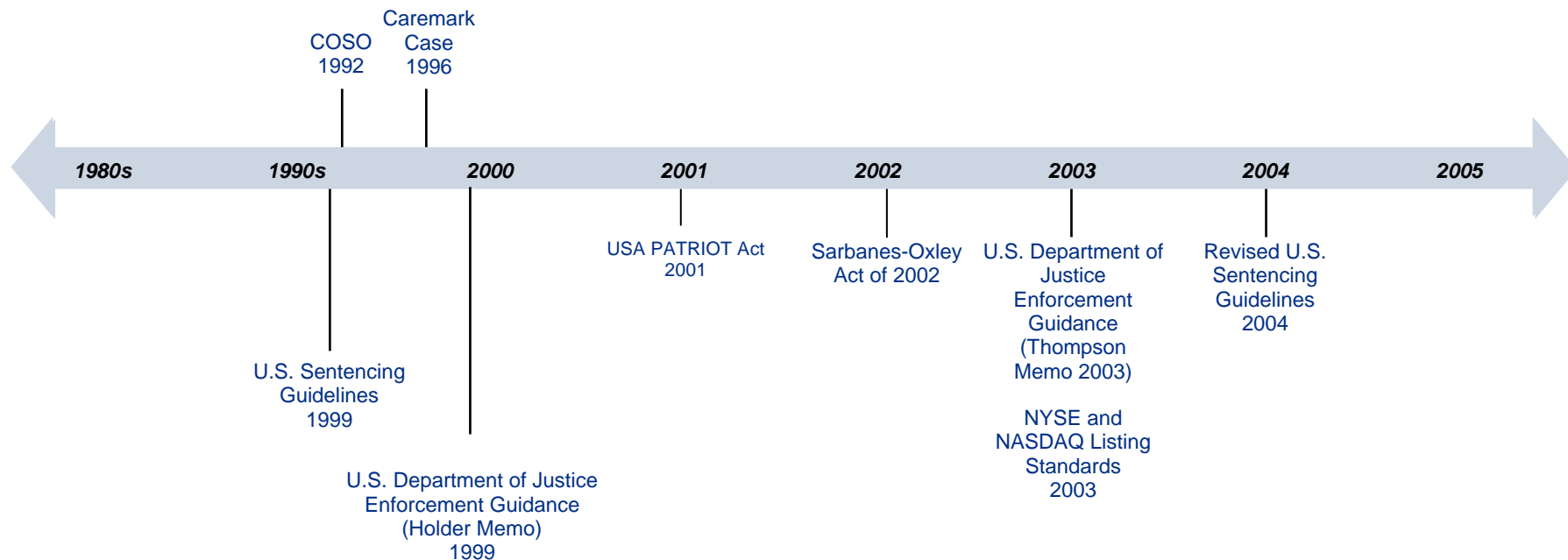
- ◆ Why perform a formal compliance risk assessment ?
  - The learning objective is to provide an understanding of why the current regulatory and competitive landscape requires organizations to undertake a compliance risk assessment
    - Regulatory influences
    - Benefits to the organization

# Why Perform a Formal Compliance Risk Assessment?

## Regulatory Influences

- ◆ U.S. Federal Sentencing Guidelines requirement
- ◆ Strongly recommended by OIG/AHLA guidance for healthcare boards
- ◆ Thompson and McNulty memos
- ◆ Boards have a heightened awareness and liability post Enron/Worldcom/SOX

# Convergence of Regulatory Challenges: A Time Line



# Benefits of a Formal Compliance Risk Assessment

- ◆ You don't know what you don't know
- ◆ Gets the attention and interest of top management and the Board (interviewees)
- ◆ Indirectly provides compliance training for top management and the Board
- ◆ Post Enron/WorldCom/SARBOX Board members are significantly more concerned about their personal liability and responsibility as Board members
- ◆ Board members don't want to be viewed as willfully ignorant or condoning

# If You Are Still in Doubt...

- ◆ U.S. Federal Sentencing Guidelines Culpability Score and resulting fines/penalties will significantly increase if your organization is deemed to not have an effective compliance program
- ◆ You should be able to answer “Yes” to the following questions:
  - Did your organization incorporate and follow applicable industry practices?
  - Was the Compliance program given adequate resources?
  - If your organization is large did you devote more formal operations and greater resources in meeting the requirements than a small organization?
  - Did your organization perform a periodic risk assessment and develop a risk assessment tool which is re-evaluated on a regular basis to ensure you are addressing specific industry high risk areas?

# Still Not Convinced?

- ◆ Perform a cost benefit analysis
  - Compare the cost of having an outside expert help your organization perform a proper risk assessment .... Versus the increase in fines/penalties if the DOJ/OIG determines you do not have an effective compliance program

# Make or Buy?

- ◆ Short Answer – Both

- ◆ Buying

- Good business practice is to periodically have outside independent experts perform a formal compliance risk assessment which provides:
  - More credibility with the Board and top management
  - Multiple, independent and varied expert resources – a fresh look
  - Results - auditing and monitoring compliance plan

# Make or Buy?

## ◆ Make

- In interim periods, use the methodology and format used by the outside experts to perform annual compliance risk assessments with internal compliance personnel
- Tag-along with the outside experts during the formal risk assessment to learn how they conduct the interviews
- Copy the experts: Don't re-invent the wheel

# Chapter 2

- ◆ How to develop organizational support and sponsorship
  - The learning objectives are to provide understanding of key organizational dynamics that enhance or serve as obstacles to getting this process approved and implemented
    - Past experiences
    - Timing
    - Available resources
    - Alignment with key organizational objectives
    - Budgeting & other considerations

# Developing Organizational Support

## ◆ Past Experiences to Consider

- Is this the first risk assessment ?
- What is the organizational appetite for risk assessment ?
- When was the last risk assessment ?
- How was the last one received ?
- Were you the person that initiated the last one ?
- Is the same management team at the helm ?
- Did the organization effect necessary change ?
- Do you sense great organizational resistance ?

# Developing Organizational Support

## ◆ Timing

- Where are you in the fiscal year ?
- Are there competing initiatives ?
- Are there other outside initiatives ?
- Are key players going to be available ?
- What is the attention span of the organization ?
- When are the next board meetings ?
- Are there any major internal inquiries ongoing ?

# Developing Organizational Support

## ◆ Available resources

- What is the availability of internal participants ?
  - The Board, CEO, CFO, COO, GC, Med Director, others
- If performing the assessment internally, do you have:
  - Independent objectivity ?
  - Knowledge to establish a broad risk profile ?
  - An understanding of the relative risks ?
  - The availability of a regulatory resource ?
  - A methodology that has been validated ?
  - The time to perform the assessment ?
  - The organizational presence ?
  - The interview skills ?
  - The facilitation skills ?

# Developing Organizational Support

- ◆ Alignment with key organizational objectives
  - Where is the organization from a strategic perspective ?
  - Is the organization pro-active or re-active ?
  - Is your program a “real” program ?
  - Is your organization obsessed with growth ?
  - Are you included in key strategic planning sessions ?
  - Do you *really* have support from the top ?
  - Do you *really* have the resources you need ?
  - Are your compliance committee meetings well attended ?

# Developing Organizational Support

- ◆ Budgeting and other considerations
  - How much can you spend on external consultants ?
    - You get what you pay for – make sure you get what you *need*
  - Do you have the resources you need to do it internally ?
    - Regulatory resource / internal counsel / access to counsel
  - Be careful what you ask for....you may find it!
  - Now what ?
  - Is the organization ready for required next steps ?

# Chapter 3

- ◆ How to conduct a compliance risk assessment
  - The learning objective is to provide an understanding of key steps to designing and implementing an effective risk assessment
    - Planning and kick off
    - Document review
    - Conducting management interviews
    - Rating and ranking methodologies
    - Compiling the risk profile
    - Analyzing and sharing the data
    - Prioritizing the risk profile

# Conducting the Risk Assessment

- ◆ Planning and kick off
  - Scheduling interviews
    - How much time do you need and when do you need it ?
  - Targeting the right areas (80/20)
  - Effectively communicating the objectives
    - Who, what, why, where, when
    - What do you need ME to do ?
  - What is your plan and how are you staying on plan ?
  - Consistent treatment across the board
  - Ensuring people are prepared when you arrive
  - Privilege or not privilege ?
  - If external – how should you be involved ?

# Conducting the Risk Assessment

## ◆ Document review

- Why do you need to review documents ?
- What documents do you need ?
  - Previous audits
  - Hotline reports
  - External evaluations
  - Previous risk assessment reports
  - Documentation of controls
  - Corrective action plans
  - Policies and procedures
- Detail or high level review ?

# Conducting the Risk Assessment

- ◆ Conducting management interviews
  - Who do you need to speak with ?
    - Alone or assisted ?
  - Communicating the objectives
  - Ensuring the interviewee is prepared
  - A level playing field....if you build it they will come
  - Are you a capable interviewer ?
  - What are you going to ask ?
  - Asking the tough questions
  - Getting a tough answer
  - Keeping the conversation on track and meaningful

# Conducting the Risk Assessment

- ◆ Rating and ranking methodologies
  - Consistency is critical
  - Likelihood of the risk
  - Significance or impact if the risk occurs
  - Mitigating factors to consider
  - Red, Yellow, Green
  - One through Ten
  - High, Medium, Low
  - Embracing the organizational vernacular

# Conducting the Risk Assessment

- ◆ Compiling the risk profile
  - How to organize the data
    - By functional area
    - By risk categories
    - By High, Medium, Low
    - All of the above ?
    - None of the above ?

# Conducting the Risk Assessment

- ◆ Analyzing and sharing the data
  - Understanding the data
  - Anticipating the reaction to the data
  - Is this really what you said ?
  - Is this really what you meant ?
  - Who needs to see the results (at this point) ?
  - Avoiding data overload

# Conducting the Risk Assessment

## ◆ Prioritizing the risk profile

- So many risks...so little time
- Which high risks are really high risks ?
  - Why is THAT a high risk ?
  - What does high risk really mean ?
  - He said low risk, she said high risk...now what ?
  - Understanding your vulnerabilities
  - Protecting the innocent

# Chapter 4

- ◆ Reporting the results: Leadership and the Board
  - The learning objective is to understand how to properly lay the groundwork for presenting the findings
    - Understanding potential pitfalls
    - Reporting to interviewees
    - Reporting to your compliance committee
    - Reporting to executive leadership
    - Reporting to the Board
    - Selling the message to the Board
    - Obtaining necessary endorsements and resources

# Reporting the Results

- ◆ Understanding potential pitfalls
  - Vetting the data – “I didn’t say that”
  - Changing of the guard
  - The messenger
  - You can’t “*unring* the bell”
  - I am trying to run a business here
  - Now what do you want me to do ?

# Reporting the Results

## ◆ Reporting to interviewees

- When will I see the report ?
  - You may or may not
- What do you need me to do next ?
  - Please stand by
- Keeping constituents appropriately informed
  - Big picture objective
  - Probable next steps
  - Specific responsibilities

# Reporting the Results

- ◆ Reporting to your compliance committee
  - Vetting the data
  - Distilling key information
  - Strategic planning of next steps
    - What are realistic objectives ?
    - What are you trying to achieve ?
    - How are you going to get there ?
  - Setting time frames for next steps

# Reporting the Results

- ◆ Reporting to executive leadership & the Board
  - Understanding the dynamics
  - Understanding the big picture
  - Understanding your obligations and responsibilities
  - Real life examples
  - What are the implications ?
  - What do you need me (us) to do ?
  - What if it does not go well ?
    - What's your back up plan ?
  - Educating the Board
  - Getting commitment on next steps

# Chapter 5

- ◆ Corrective action planning and implementation
  - The learning objectives will be to provide an understanding for necessary steps to manage the identified risks
    - Establishing accountability
    - Trust but verify....What's your corrective action plan ?

# Corrective Action Planning and Implementation

## ◆ Establishing accountability

- Who owns it ?
- Who controls it ?
  - Understanding “upstream and downstream implications”
- Where is it broken ?
- Documenting the ownership

# Corrective Action Planning and Implementation

- ◆ Trust but verify .... What's your corrective action plan ?
  - Where is it broken ?
  - Policy and procedure development
  - Developing and delivering effective training
  - Developing and implementing auditing and monitoring plans



# Questions?

# Contact Information

**Ken Zeko**

KPMG LLP

[kzeco@kpmg.com](mailto:kzeco@kpmg.com)

214-840-6497

**Joel Dziengielewski**

KPMG LLP

[jdziengielewski@kpmg.com](mailto:jdziengielewski@kpmg.com)

212- 954-3884

**Scott Remmich**

Triad Hospitals, Inc.

[scott.remmich@triadhospitals.com](mailto:scott.remmich@triadhospitals.com)

214-473-7028

**Phil Eubanks**

Memorial Hermann  
Healthcare System

[phil.eubanks@memorialhermann.org](mailto:phil.eubanks@memorialhermann.org)

713-448-4188

**All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.**