



## Assessing Compliance Priorities: Considerations for Conducting an Effective and Collaborative Compliance Risk Assessment

October 25, 2023

Noah Goldstein, JD

Sara Simon, JD

# Opening Disclaimer

The views expressed by all of us are merely personal opinions. They do not necessarily reflect the views of our current or past employers.

Nothing we say should be considered legal advice.



# Why Conduct a Compliance Risk Assessment?



Always better to be proactive vs. reactive



Identifies compliance risks



Allows for prioritization of risk areas



Evaluates the effectiveness of existing compliance program/framework



Identifies gaps in compliance



Facilitates allocation of resources



Government recognition (“credit”) in the event of investigation

# Major Risk and Enforcement Areas for Life Sciences Companies




FDA

Kickbacks

False Claims

Privacy



## 7 Elements of an Effective Compliance Program (2003 OIG Compliance Program Guidance for Pharmaceutical Manufacturers)

- Designated compliance officer and compliance committee; senior management involvement
- Written policies and procedures
- Training
- Open communication; raising concerns/issues
- Response to compliance concerns/corrective action
- Enforcement of written policies/standards
- Internal audits/monitoring





# DOJ Guidance for Evaluating Corporate Compliance Programs (updated 3/23)

## ➤ DOJ's expectation

- An effective corporate compliance program should evaluate risks on an ongoing basis in light of the following questions:
  - *Is the company's compliance program well designed? \*\**
  - *Is the program being applied earnestly and in good faith? Is it adequately resourced and empowered to function effectively ?*
  - *Does the company's compliance program work in practice?*

*\*\* more about this later*

*"Even a well-designed compliance program may be unsuccessful in practice if implementation is lax, under-resourced, or otherwise ineffective. Prosecutors are instructed to probe specifically whether a compliance program is a 'paper program' or one implemented, resourced, reviewed, and revised, as appropriate, in an effective manner."*

# 30,000 Foot View . . .

## ➤ Questions to ask:

- Are we considering the right risks?
- Are/how are we limiting risks?
- Are we mitigating risks/preventing them from reoccurring?



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

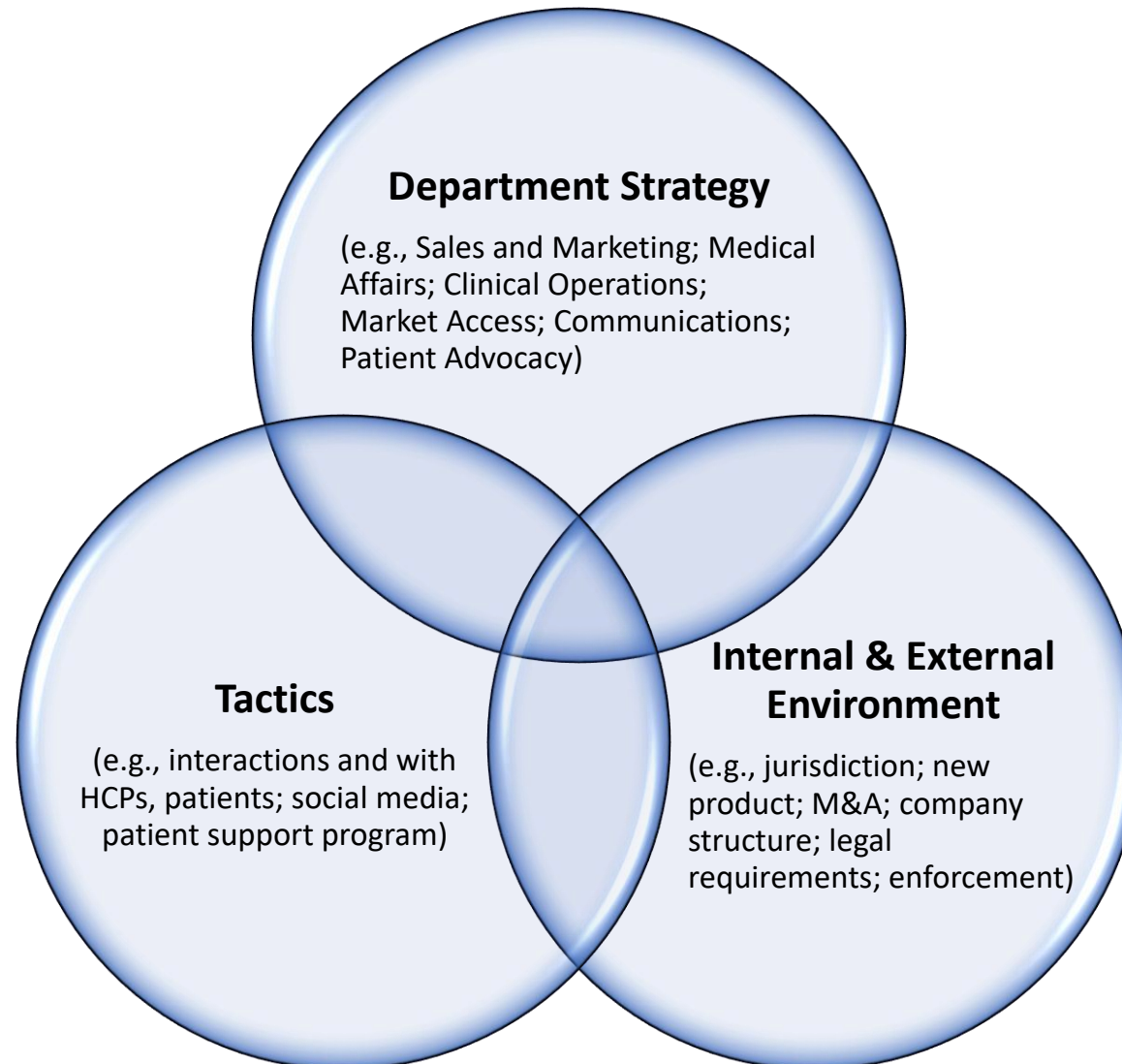


# Planning for a Risk Assessment

- Identify areas to be addressed
  - Enterprise compliance risk or focused risk areas (i.e., HCP engagement, Transparency/Sunshine, Privacy etc.)
- Consider methodology & approach
  - Document review
  - Interviews with stakeholders
  - Consideration of past identified risk areas/history of compliance violations
  - Budget and resource considerations/need buy-in from senior leadership/project manager (need one “point person”)
- What is your deliverable and how/who/where will it be shared?



# Understanding the Business



# Assessing your Current State (of compliance)

How is Compliance  
viewed by the  
organization?

Do you have a  
compliance program  
structure in place?

Do you have a Code of  
Ethics?

Do you have  
policies/procedures?

Has training been done  
at all levels (including  
the Board level &  
Senior Management)?

Are employees aware  
of the rules?

Do employees  
understand the rules?

Do you have review  
committees?

# DOJ Risk Assessment Analysis

*“Prosecutors should also consider ‘[t]he effectiveness of the company’s risk assessment and the manner in which the company’s compliance program has been tailored based on that risk assessment’ and whether its criteria are ‘periodically updated.’”*

## Risk Management Process

- *What methodology/metrics has company used to identify, detect and address risks?*

## Risk-Tailored Resource Allocation

- *Does company devote the appropriate amount of time to the correct risk areas?*

## Updates and Revisions

- *Is the risk assessment current/subject to periodic review? Is it just a snapshot in time? Has the review led to updates in policies, procedures and controls?*

## Lessons Learned

- *Does the company have a process for tracking lessons learned from its own issues or from other companies’?*

# Developing a Compliance Risk Matrix

Identify risks

Prioritize and measure risk based on:  
-Probability of occurrence  
-Severity of Impact

Evaluate/Confirm appropriate controls or strategies to minimize the risk

The structure of your company will likely drive your risk profile

Use as a tool in the decision-making process

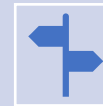
**RISK ASSESSMENT**

IMPACT	↑	Significant	Considerable Management Required	Must Manage and Monitor Risks	Extensive Management Essential		
			Moderate	Risks May be Worth Accepting with Monitoring	Management Effort Worthwhile	Management Effort Required	
				Low	Acceptable Risks	Accept and Monitor Risks	Manage and Monitor Risks
					Low	Moderate	High
			LIKELIHOOD →				

# Developing Priorities and Timelines



How will the “results” of the risk assessment be communicated within the company?



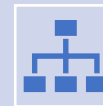
What will the company do to manage the risk(s) (policies, training, monitoring, etc.)?



What resources does the company have to manage the risk?



When will implementation take place?



What role will everyone play?



# Hypothetical #1

You are a compliance attorney at a growing company that is about 10 months away from receiving FDA approval of its first product. You are responsible for leading the build of the company's compliance program and you think that it would be prudent to conduct a company-wide healthcare compliance risk assessment to assess the company's current and future potential risks and evaluate its needs.

- **What (additional) considerations, if any, are necessary to contemplate as the company approaches commercialization?**
- **How would you begin the risk assessment process?**

# Hypothetical #2

Your company, which is subject to transparency reporting and disclosure requirements, has just acquired another company what is also subject to these requirements. As you look to integrate operations you have determined that it would be helpful to conduct a transparency risk assessment to assess each company's compliance approach with these requirements.

- **How would you approach this risk assessment?**
- **Which individuals at your company do you think you will need to get onboard, or buy-in from to be able to effectively conduct this assessment?**

# Potential Benefits of doing a Compliance Assessment



Compliance efforts  
become more  
effective



Reduce  
Legal/Compliance  
Risk



Save \$\$\$ (Legal fees,  
penalties, settlement  
costs)



Improve Reputation



Improve company  
culture



Manage and mitigate  
existing and new risk  
areas



WILL HELP YOU SLEEP  
AT NIGHT

# Questions/Ideas?

