Compliance Summer School: Demystifying Risk Assessments and Audits

July 11, 2023
3:00 pm – 4:00 pm CT

Presented by:
Amanda Johnston, JD, RAC
Managing Attorney
Gardner Law, PLLC

GARDNER LAW

Introduction

Amanda Johnston, JD, RAC, Managing Attorney, Gardner Law, specializes in counseling medical technology and pharmaceutical companies on FDA law, regulatory submissions and strategy, healthcare compliance programs, and fraud and abuse laws. Prior to practicing at Gardner Law, she was the Compliance Officer at Coloplast Corp, in Regulatory Affairs at Medtronic (Star of Excellence Award winner), and in Compliance at UnitedHealth Group. Amanda is an Adjunct Professor of Law at Mitchell Hamline School of Law where she teaches Drug & Device Law.

Amanda Johnston, J.D.,
R.A.C. Managing Attorney
ajohnston@gardner.law
Mobile: 763-639-6951

Agenda

- Compliance Program Refresher
  - 7 Elements of an Effective Compliance Program
  - Bonus 8th element
- Compliance Risk Assessments
- Compliance Audits
- Best Practices, Tips & Tricks
- Pitfalls & Watch outs

GARDNER LAW

What is a Compliance Program?

- A compliance program is more than just policies and procedures.
- It is an infrastructure of rules, training, penalties, and response protocols designed to promote the prevention of misconduct, reduce the incidence of noncompliance to laws, detect noncompliance faster when it does happen, and prevent it from happening again.
- FDA-regulated companies are subject to many complex laws, and compliance with those laws will not happen by chance.

7 Elements of an Effective Compliance Program

1. Implementing written policies, procedures and standards of conduct;
2. Designating a compliance officer and compliance committee;
3. Conducting effective training and education;
4. Developing effective lines of communication;
5. Conducting internal monitoring and auditing;
6. Enforcing standards through well-publicized disciplinary guidelines; and
7. Responding promptly to detected offenses and undertaking corrective action.

GARDNER LAW

BONUS 8th Element: Compliance Risk Assessment

- What is a risk?
  - A situation associated with a particular region, business activity, or product that can present a greater possibility for non-compliance with policies and procedures, and government laws, regulations, and requirements.

- What is a compliance risk assessment?
  - A structured approach to identifying and defining risks for an organization to facilitate a targeted compliance program to focus essential resources on the most significant risks.

Why Conduct a Risk Assessment?

- Regulators expect it.
  - U.S. Federal Sentencing Guidelines:
    - "In implementing [a compliance program], the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth…to reduce the risk of criminal conduct identified through this process."
  - DOJ's "Evaluation of Corporate Compliance Programs" (last updated March 2023):
    - "The starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks."
    - "For example, prosecutors should consider whether the company has analyzed and addressed the varying risks presented by, among other factors, the location of its operations, the industry sector, the competitiveness of the market, the regulatory landscape, potential clients and business partners, transactions with foreign governments, payments to foreign officials, use of third parties, gifts, travel, and entertainment expenses, and charitable and political donations."

Why Conduct a Risk Assessment?

- Efficiency; focus resources on high risks
- Find blind spots
- Demonstrate proactive approach to compliance
- Employee engagement
- Builds a culture of compliance

How to Conduct a Compliance Risk Assessment

- There is no one-size-fits-all process.
- The approach should be tailored to the company's size, maturity, business activities, etc.

Example Compliance Risk Assessment Process

1. Define objectives and scope

- Create Risk Assessment Plan
- Define areas of focus: consider privacy, cybersecurity, FDA regulations, state laws
- Compliance vs. Enterprise Risk Assessment
  - Reputational harm, financial impact, business impact
- Geographic scope
- Business units
- Business activities

2. Conduct the Risk Assessment

- Consider methods:
  - Document review, 1:1 interviews, staff surveys, focus groups, external consultant
- Score/rank key risks:
  - Subjective & objective inputs
  - Likelihood/probability of occurrence
  - Severity of risk
  - Consider risks: legal, compliance, reputational, business, financial
- Output
  - Spreadsheet
  - Slide deck
  - Heat Map

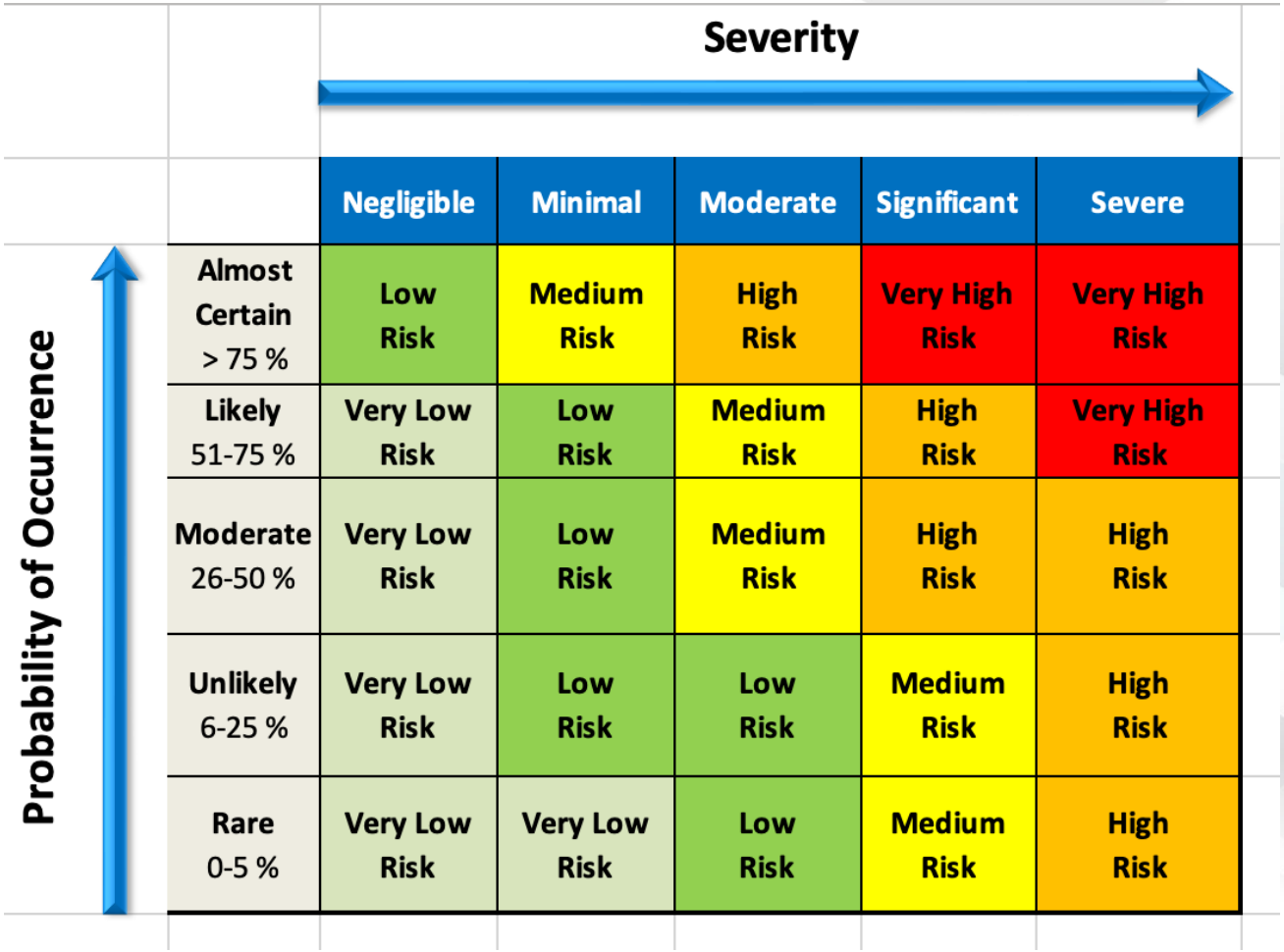
Example Risk Categories (not exhaustive)

- Promotional Speaker Programs
- Consulting Agreements
- Provision of Rebates and Discounts
- Grants
- Marketing the Spread (Reimbursement/HCEI)
- Provision of Value-Added Services
- Co-Marketing
- Provision of Free Products
- Sample Programs
- Coupon and Voucher Programs
- Patient Assistance Programs
- Promotional Speaker Programs
- Continuing Medical Education
- Off-Label Promotion (Generally)
- False or Misleading Statements
- Disease Education vs. Promotion
- Practice Building
- Minimization of Risk Information
- Unsubstantiated Product Comparisons
- Distribution of Off-Label Materials
- Publication Practices
- Press Releases
- Inducing the Submission of False Claims
- Educational and Research Grants
- Supply Chain
- Customs Brokers/Bribery
- Good Manufacturing Practice (GMP) Requirements/Inspections
- Importation Inspections and Alerts
- State Licensing
- Sponsor Monitoring
- Data Integrity Issues
- Handling of Recalls
- Post-Market Adverse Event Reporting
- Handling of Labeling Changes
- Good Clinical Practice (GCP) Requirements
- Document Retention
- Responsible Corporate Officer Liability
- Reimbursement Support/Guidance
- Patient Steering
- Handling Patient Information
- Cybersecurity
- Data Security
- Privacy (HIPAA/GDPR)

EXAMPLE Compliance Risk Matrix

Category	Risk	Description	Consequences (1-5)	Probability (1-5)	Risk Level (before controls)	V
Promotional Practices	Off-Label Promotion	Advertising and promotional materials are outdated and	3	4	Medium Risk	
Bribery/Kickbacks	Gifts to HCPs (Meals)	Meal limits are not widely known or not widely adhered to	4	3	High Risk	
Local/State Laws	State Licensing Noncompliance	Not licensed in all applicable states as a medical device manufacturer	2	5	Low Risk	
Transparency Reporting	Failure to accurate report payments for Sunshine Act	Lack of a formal tracking method to ensure that all meals/TOV to HCPs are documented internally	2	4	Medium Risk	

EXAMPLE Heat Map

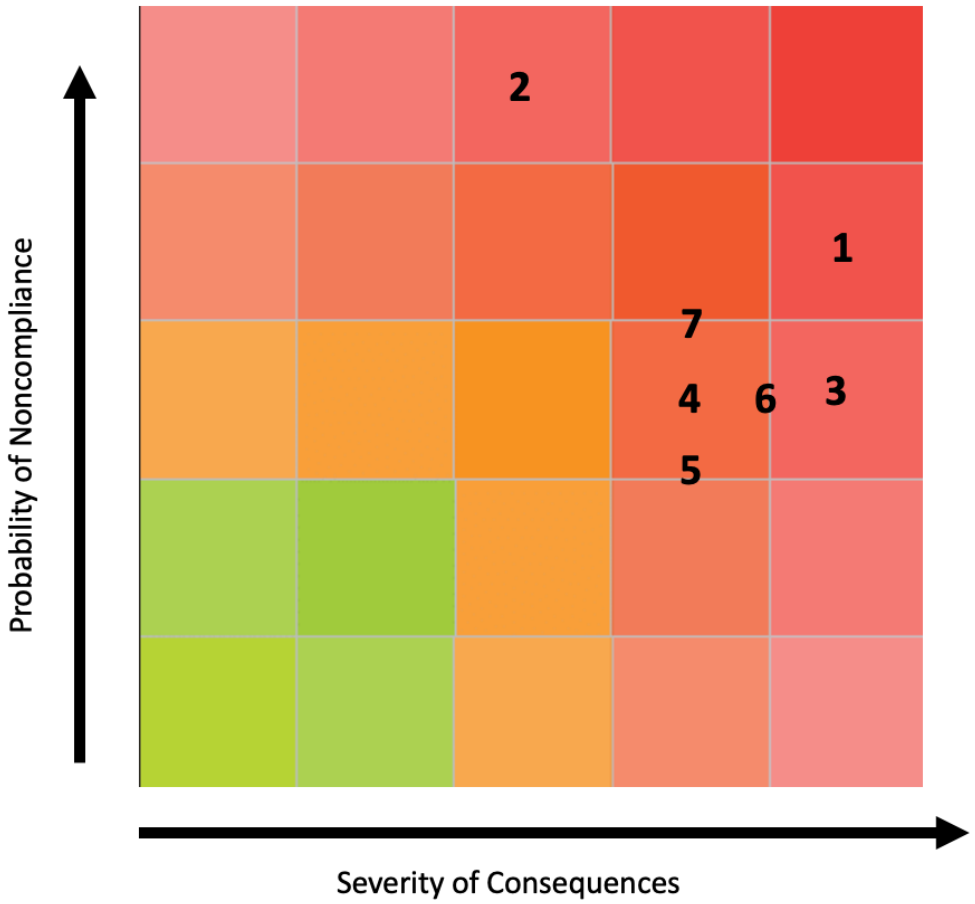


	Negligible	Minimal	Moderate	Significant	Severe
Almost Certain > 75 %	Low Risk	Medium Risk	High Risk	Very High Risk	Very High Risk
Likely 51-75 %	Very Low Risk	Low Risk	Medium Risk	High Risk	Very High Risk
Moderate 26-50 %	Very Low Risk	Low Risk	Medium Risk	High Risk	High Risk
Unlikely 6-25 %	Very Low Risk	Low Risk	Low Risk	Medium Risk	High Risk
Rare 0-5 %	Very Low Risk	Very Low Risk	Low Risk	Medium Risk	High Risk

GARDNER LAW

EXAMPLE Heat Map

1. Advertising & Promotional Practices (Off-Label)
2. Kickbacks (HCP Meals)
3. State Licensing Noncompliance
4. Third-Party Diligence
5. HIPAA/Privacy/Security
6. Transparency Reporting
7. Speaker Programs



GARDNER LAW

3. Develop & Implement Compliance Work Plan

- Develop & execute a Compliance Work Plan
  - Audit or investigation warranted?
  - Corrective actions?
- Monitor progress
  - Use a measurable method to facilitate tracking/trending over time
- Repeat
  - Continuously monitor and update
  - Formal review every 1-2 years

EXAMPLE Compliance Risk Assessment

Risk Identified (in order of risk assessment results priority)	Risk Mitigations to Consider
Lack of control over advertising and promotional materials	Review/update SOPs, document process, create central repository, training, monitor for compliance.
Improper sharing of reimbursement information/HCEI	Review/update SOPs, training, monitor for compliance
Off-label promotion	Review/update SOPs, training, monitor for compliance
Speaker programs	Continued training, monitor for compliance, monitor expense reports
Lacking top-down culture of compliance	Training, other compliance initiatives
Unauthorized practice of medicine	Review/update SOPs, training, monitor for compliance
State gift ban laws and limits	Review/update SOPs, training, monitor for compliance

EXAMPLE Compliance Work Plan

Risk Identified	Mitigation Plan	Person Responsible	Timeline
Priority Level 1			
Lack of control over advertising and promotional materials	Review/update SOPs, document process, create central repository, training, monitor for compliance.	John Doe	Immediate action (complete by Q3 2023)
Priority Level 2			
Improper sharing of reimbursement information/HCEI	Review/update SOPs, training, monitor for compliance	Jane Doe	Complete by Q3 2023
Off-label promotion	Review/update SOPs, training, monitor for compliance	John Doe	Complete by Q3 2023
Speaker Programs	Continued training, monitor for compliance, monitor expense reports	John Doe	Complete by Q3 2023
Priority Level 3			
Unauthorized practice of medicine	Review/update SOPs, training, monitor for compliance	Jane Doe	Ongoing, review in Q1 2024
State gift ban laws and limits	Review/update SOPs, training, monitor for compliance	Susie Doe	Ongoing, review in Q1 2024

EXAMPLE Work Streams

- Advertising and Promotional Materials Review Workstream:
  - Activity 1: Conduct an audit
    - Team:
    - Timelines:
  - Activity 2: Document process, review/update SOP
    - Team:
    - Timelines:
  - Activity 3: Create a central repository
    - Team:
    - Timelines:
  - Activity 4: Train staff on the updated process
    - Team:
    - Timelines:

Risk Assessments: Best Practices, Tips & Tricks

- Educate & engage staff
- Consider software/technology support
- Include objective and subjective inputs
- Consider external support
- Ensure knowledge of applicable laws, industry climate, and enforcement trends
- Ensure alignment on the risk rating approach and risk tolerance levels in advance
- Acknowledge that there is inherent risk in some areas and activities
- Risk assessment activities could drive audits or even investigations

Risk Assessment: Pitfalls, Watch Outs

- Not doing one
- You don’t know what you don’t know
- Too large of a scope
- Not properly assessing risks
- Lack of work plan or follow-up activities
- Leaving out levels or departments

Compliance Audits

- One of the original 7 elements
- Separate from risk assessment, but related in that risks should drive audits
- You need knowledge of the risks before you conduct an audit

- Compliance audit:
  - A focused, systematic, and independent examination of a company's processes, operations, and activities to assess whether they adhere to applicable laws, regulations, industry standards, and internal policies.

Audit vs. Risk Assessment

	Compliance Audit	Compliance Risk Assessment
Purpose	Evaluate a company's compliance with laws, regulations, and policies.	Identify and evaluate potential compliance risks that an organization may face. Involves assessing the likelihood and impact of compliance failures.
Focus	Narrow scope, looking back	Broad scope, looking at present and ahead
Timeframe	Periodic, limited	Continuous
Output	Audit report	Work plan

Compliance Audits: Best Practices, Tips & Tricks

- Take a risk-based approach
  - Use the risk assessment
  - Current enforcement/industry trends
- Maintain objectivity and independence
- Create an audit plan with clear objectives, scope, and methodologies
  - Document the audit plan and report
- Gather sufficient and reliable evidence using varied audit techniques
  - Interviews, document review, data analysis, observation
- Fully document when findings are addressed (take credit)
- Recommend a comprehensive compliance audit every 1-2 years

Compliance Audit Pitfalls & Watch Outs

- Lack of proper planning and resource allocation
- “Check the box” audits
- Inadequate understanding of the risk areas and compliance requirements
- Flawed risk assessment
- Failure to address findings
- Inadequate evidence gathering for reliable findings
- Neglecting monitoring

Questions?

Thank you!

Amanda Johnston, J.D., R.A.C.
Managing Attorney
ajohnston@gardner.law
Mobile: 763-639-6951

GARDNER LAW