ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

BUSINESS ETHICS LEADERSHIP ALLIANCE (BELA)

Where the Best Companies Come Together to Advance Business Integrity

PRESENTED BY:

Pamela Jergens
Director, BELA Engagement
pamela.jergens@ethisphere.com

DATE:

February 9, 2022

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

February 9, 2022

Antitrust Statement

One reminder: based on the agenda for our meeting, it seems unlikely that we will be discussing anything that relates to competitive practices or that is relevant under antitrust or competition laws. However, to ensure that everyone is comfortable with all aspects of the conversation, we would like to state explicitly that the conversation will not include discussions, agreements or concerted actions that may restrain competition. This includes the exchange of information concerning individual prices, rates, coverages, market practices, claims settlement practices, or any other competitive aspect of an individual company's operation. If at any time anyone feels that some aspect of the conversation may be inappropriate because of antitrust or competition laws, that person is encouraged to voice his or her concern immediately, and we will terminate that conversation and turn to other matters.

BUSINESS ETHICS LEADERSHIP ALLIANCE™
An Ethisphere Community

Wednesday, February 9, 2022

Virtual Roundtable

THANK YOU TO OUR PRESENTERS:

Cleveland Clinic

Northwell Health℠

AGENDA

1:00pm – 1:15pm	**Welcome, Rules of Engagement & Introductions**
1:15pm – 2:45pm	Risk and Resiliency: Developing Effective Compliance Risk Assessments and Processes *Discussion Leads: Greg Radinsky, CCO, Northwell Health and Don Sinko, CIO, Cleveland Clinic* • An Overview of Risk Assessment Best Practices • Leveraging Enterprise Risk Management • Tips on Collaborating with Internal Audit • Best ways to Utilize Artificial Intelligence and Traditional Data Sources • Assessing the Risk Assessment Process Maturity Level **Open Discussion and Q&A**
2:45pm – 3:00pm	**Closing Remarks**

Ethisphere BELA Roundtable

Risk and Resiliency: Developing Effective Compliance Risk Assessments and Processes

February 9, 2022

Greg Radinsky, JD, MBA
Senior Vice President
Chief Corporate Compliance Officer

Donald A. Sinko, CPA, CRMA
Chief Integrity Officer
Corporate Compliance and Business Ethics
Internal Audit

Northwell Health℠

Cleveland Clinic

Variety of Risk Assessments

Risk assessments can take many forms and we do them every day or periodically

- Go to work today?
- Should I ask the CEO that question?
- Multiple types of formal risk assessments:
  - Enterprise Risk
  - Corporate Compliance
  - Internal Audit
  - Cybersecurity
  - Quality and Safety

Polling Question

Do you participate in your organization's Enterprise Risk Management process?

(a) Yes
(b) No
(c) N/A (organization does not have an ERM Process)

Risk Assessment Basics for Compliance Officers

Michelle Cooper and Don Sinko

¶60,000 Introduction

* Every individual, including compliance officers, has conducted or participated in a risk assessment. Risk assessments occur all day long. For example, consider the following scenario:

Joe Smith woke up this morning to his alarm clock and asked himself, "Do I have a meeting first thing this morning or can I hit the snooze button?" Likely, he undertook a risk assessment to make his decision. He asked the following questions: "What do I have on my schedule today? How much work do I have to get done?" and "What would be the impact if I slept in a little longer?" Once he assessed the impact, he probably considered how his day would be affected by his decision - how often he slept in previously, how likely his tardiness would be noticed, his ability to correct the result of his tardiness before it was realized by others?

Joe just conducted a risk assessment. As will be described later in this chapter, Joe just evaluated the inherent risk of the activity (or lack thereof). He also evaluated the controls he had in place to mitigate the risk. First, he may have hit that trusted snooze button a couple of times. He also may have evaluated the residual risk, the amount of risk that exists after internal controls are in place. Joe may have determined the level of risk impact, his vulnerabilities, and evaluated the current control environment in light of the risk. Based on this risk assessment, he may have decided to sleep only until the next alarm sounds or he may have decided to get out of bed and get ready for work.

An effective method for discovering and evaluating an organization's compliance risk areas is to perform a compliance risk assessment. In the Office of Inspector General's (OIG) Compliance Program Guidance for Hospitals, the OIG recommends that when creating a compliance plan, the compliance officer, with help from the department managers, should take a snapshot of operations from a compliance perspective. The OIG then suggests that this "snapshot become a benchmark baseline for the compliance officer or others to judge the organization's progress in reducing or eliminating potential areas of vulnerability.[1]

Risk assessments take many forms. They can take the form of a simple gap analysis or a complicated underwriting evaluation. The risk process may be formal and occur only once a year or quarterly or on an as needed basis. A risk assessment is simply a mechanism used to identify and evaluate key exposures (vulnerabilities or weaknesses) and establish plans for mitigating overall organizational risks.

Compliance officers are charged with developing and overseeing the compliance risk assessment process. Because compliance officers come from varying backgrounds, the approach to developing a risk assessment program will vary based upon previous experience, training, and organizational resources.

This chapter will provide the elements of an effective risk assessment program, provide methodologies, tools, and resources for implementing and operating a risk assessment program, and recommendations for effective implementation.

¶60,005 Definitions

Some key definitions are a good starting point. There are many variations of the definitions below, but for purposes of this chapter, the following defi-

---

* Michelle Cooper and Donald A. Sinko, updated this chapter for publication in this manual for the December 2020 quarterly report. This chapter was originally written by A. Michelle Cooper, MS, CPA, Executive Vice President and Chief Compliance Officer of CommonSpirit Health (CommonSpirit) and Margaret Hambleton, MBA, CHC, CHPC.

Michelle is responsible for compliance, contracts administration, privacy, and information security oversight for the system. She is active in a variety of professional organizations and is a frequent speaker on healthcare compliance, leadership, ethics, compliance risk and internal control topics. She is also a Co-Chair of the American Hospital Association (AHA) Chief Compliance Officer Roundtable.

Donald A. Sinko, CPA, CRMA, Chief Integrity Officer for Cleveland Clinic, is responsible for the office of Internal Audit and the office of Corporate Compliance and Business Ethics, with dotted-line oversight of information security. He is active in a variety of professional organizations and is a frequent speaker on healthcare compliance, leadership, ethics, risk management and process control topics. He is also a Co-Chair of the AHA Chief Compliance Officer Roundtable.

[1] OIG Compliance Program Guidance for Hospitals, February 1, 1998.

Identifying Areas of Risk

- Interviews of key personnel, including the Board
- Open-ended surveys
- Compliance hotline reports
- Employee exit interviews
- External work plans from OIG and OMIG
- Prevalent industry topics
- Internal data mining, through third party software
- Prior year audits / internal audit reports

Polling Question

Do you collaborate with Internal Audit as part of your risk assessment process?

(a) Yes
(b) No
(c) N/A (Compliance/Internal Audit same department)

Polling Question

Do you use artificial intelligence as part of your risk assessment process?

(a) Yes
(b) No

Typical Open-Ended Survey Questions

- What risks keep you up at night?
- What do you think are the top ten compliance risks?
- Are there processes or procedures you are aware of that you are not comfortable with?
- What is the number one compliance risk we should focus on?

Questions for Group Discussion

Who has done an enterprise risk assessment in the past year?

- How did you accomplish in light of work-from-home situation?
- What new data inputs have you used recently?

What about a targeted risk assessment?

- Risk-specific, Regional or Business Unit?
- Strategy employed for that decision and execution

Let's discuss experiences with top-down and/or bottom-up methodology?

- What has worked well for you in the past? Lessons learned?

Categorizing Identified Risk Areas

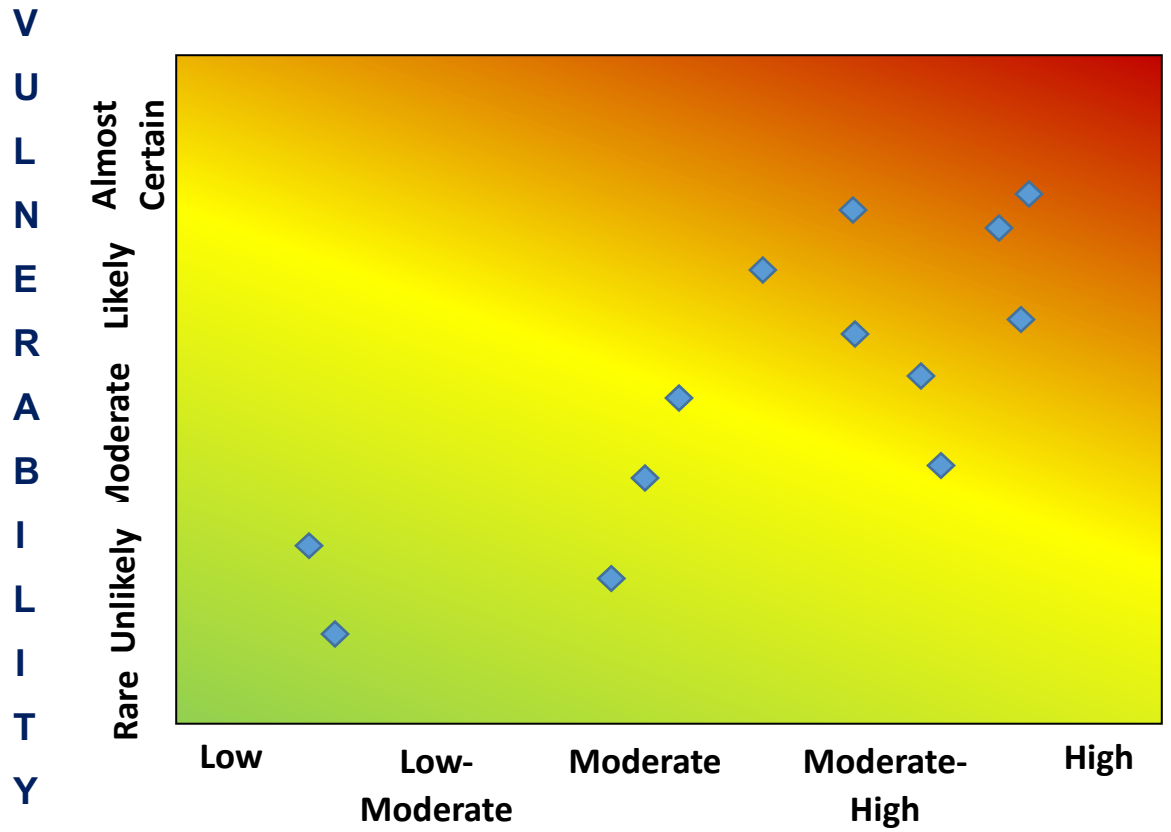
Risks can be categorized by enterprise risk area, and then compliance risk area:

- Cybersecurity
  - ➢ Privacy
- Operations
  - ➢ FCPA
- Strategic
  - ➢ Anti-trust

Prioritizing Identified Risks

- For each risk:
  - ➢ What is the likelihood of it happening?
    - Vulnerability rating
  - ➢ What is the impact if it does happen?
    - Severity rating
- Risk scoring to determine the rating
- Classify as high, medium, low

Sample Risk Heat Map



Risk Tolerance

Senior management and the Board need to identify:

- Organization's appetite for risk
- How the risk should be prioritized

Risk tolerance can range from total avoidance to total acceptance

Risk Appetite

Risk Appetite needs to consider the following:

- Psychological considerations
  - ➢ Comfort with the risk
- Cultural considerations
  - ➢ Impact on mission and values
- Strategic considerations
  - ➢ Impact on strategic initiatives
- Capacity considerations
  - ➢ Resources available

Risk Assessment Resource Guide

Compiled semi-annually and the areas covered include:

- The status of ongoing Compliance initiatives
- Key changes and updates to pertinent rules and regulations
- Risk profile chart
- Financial data and benchmarks

Risk Assessment Resource Guide (cont.)

- Government audits and trends
- Internal audits conducted
- Voluntary regulatory disclosures
- Industry developments
- Compliance Help-Line trend analysis

Polling Question

How would you rate the maturity of your risk assessment process?

(a) Very Mature
(b) Mature
(c) Average
(d) Still working on it

Questions for Group Discussion

Once your risk assessment is complete, what comes next?

- How have you developed prioritized mitigation plans and achieved buy-in from the business?
- How do you track program initiatives resulting from the risk assessment?
- What is the cadence for the next assessment? Enterprise and/or targeted?

What are some emerging risks you are monitoring/considering in 2022?

Thank You!

Greg Radinsky, JD, MBA
Senior Vice President
Chief Corporate Compliance Officer
gradinsk@northwell.edu

Donald A. Sinko, CPA, CRMA
Chief Integrity Officer
Corporate Compliance and Internal Audit
sinkod@ccf.org