Compliance Risk Assessment and Management Workshop

Society of Corporate Compliance and Ethics and
Health Care Compliance Association

1

1

II. Identification of Compliance Risk

Greg Triguba, JD, CCEP, CCEP-I

2

2

Session Agenda

II. Identification of Compliance Risk

- Understand Organizational Risks and Define Universe
  - Risk Identification - *Overview*
  - Things that Affect Risk
  - Defining Inherent, Control, & Residual Risks
  - Internal and External Inputs
- Compliance Risk Inventory
  - Key Practice Considerations
  - Methods to Identify Risk
  - Top Compliance & Ethics Risk Areas
  - Connecting Compliance Risks to ERM
- Effects of Intentional vs. Unintentional Risk Events
- Risk Identification – *Key Takeaways*

Understand Risks & Define Universe

Identification of Compliance Risk – *Understand Risks & Define Universe*

Risk Identification - *Overview*

- ✓ Important first step in the Risk Management process
- ✓ Essential to identify, define, and understand the organization's Risk Universe/Profile – *Consider Uniqueness*
- ✓ Understand what affects risk and leverage internal/external inputs
- ✓ Assure effective methods and processes are in place to identify existing, new, and emerging risks; *dynamic, evolving, and supports continuous improvement*
- ✓ Create and maintain a comprehensive Risk Inventory to capture and document a comprehensive listing of compliance risks; *classify, group and prioritize risk listing*
- ✓ Engage and collaborate with leadership and other risk management functions in the organization; *provide ongoing partnership and compliance risk input*

Identification of Compliance Risk – *Understand Risks & Define Universe*

Things that Affect Risk

- Organizational Culture
- Global operations, differing cultures, and third party relationships
- Financial and other related business demands
- Technology – *Internal/External*
- Economic Conditions/Competition/Consumer Demand
- Business strategy, decision-making, and other business objectives
- Company Incentive Programs/Performance goals

Identification of Compliance Risk – *Understand Risks & Define Universe*

Things that Affect Risk (*Cont.*)

- Mergers/Joint Ventures/Acquisitions/Alliances
- Laws/Rules/Regulations
- Emerging trends and industry practices
- Leadership/Management changes and turnover
- Political environments globally
- Unknowns (*e.g., global pandemics/emergencies, supply chain disruptions*)

Other…

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

7

Identification of Compliance Risk – *Understand Risks & Define Universe*

Defining Inherent, Control, & Residual Risks

Inherent Risk	**"The risk to an entity in the absence of any direct or focused actions by management to alter its severity."** Enterprise Risk Management – Integrating with Strategy and Performance ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.
Control Risk	**"Probability of loss resulting from the malfunction of internal control measures implemented to mitigate risks."** DifferenceBetween.com; (https://www.differencebetween.com/difference-between-inherent-risk-and-vs-control-risk/)
Residual Risk	**"The risk remaining after management has taken action to alter its severity."** Enterprise Risk Management – Integrating with Strategy and Performance ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

Examples…

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

8

Identification of Compliance Risk – *Understand Risks & Define Universe*

Internal Inputs - *Examples*

- Management input, surveys, interviews
- Business strategy, objectives, and decision-making
- Internal Audit and other functional Risk Management efforts/output
- Past internal incidents, investigations, audits, risk profiles
- Metrics and output from Reporting Mechanisms/Hotlines
- Business operations, operating locations, etc.
- Technology, Security, and other functional areas

Other…

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

9

Identification of Compliance Risk – *Understand Risks & Define Universe*

External Inputs - *Examples*

- Legal/Regulatory requirements
- Enforcement trends and activity
- Social Media and market-place trends
- Third-Party Relationships
- Industry benchmarking and practices
- Industry publications, government-issued guidance, news media
- Cultural considerations

Other…

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

10

Risk Identification – *Scenario #1*

11

Risk Identification - *Scenario #1*

A large, global medical device company recently renewed a contract with a preferred third-party vendor in Asia that supplies 90% of the rubber needed for its manufacturing operations. Recently, the vendor made headlines for its laxed labor practices and is known for taking shortcuts when it comes to adhering with global environmental standards.

Because the vendor's product is critical to the business and pricing is significantly lower than its competitors, leadership is comfortable overlooking the bad press and does not want to do anything to disrupt the supply chain or damage the vendor relationship.

What potential risks, issues, and considerations come to mind?

12

Risk Identification - *Scenario #1*

Risks, Issues, and Considerations – *Discussion*

13

13

Compliance Risk Inventory

14

14

Identification of Compliance Risk – *Risk Inventory*

Key Practice Considerations:

- Essential to have strong risk identification infrastructure in place, to include methods and practices to effectively identify and manage a dynamic/changing risk universe unique to the business; *proactive and ongoing*.
- Create and maintain a comprehensive compliance Risk Inventory listing of all key compliance risks facing the organization, to include classifying and grouping risks in the following ways:
  - *Risk type, sub-categories of risk, geographic locations/regions, division, business unit, functional areas, operations, activity, etc.*
- Rank and prioritize risk listing based on findings from the most recent assessment and other inputs, and add new/emerging risks as needed - *provides focus on the most important compliance risks*.
- Leverage technology; create Risk Inventory listings that are sortable, scalable, and provide flexibility in the level of granularity that may be needed for assessment, management, and reporting efforts.

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

15

Identification of Compliance Risk – *Risk Inventory*

Methods to Identify Risk - *Examples*

- ✓ Management Interviews
- ✓ Surveys/Focus Groups; *risk identification and culture*
- ✓ Checklists of common company/industry risks, regulatory requirements, etc.
- ✓ Establish/leverage business-level compliance committees, liaisons, ambassadors
- ✓ Review past Risk Assessments, incidents, and investigations
- ✓ Assess data/metrics from Reporting Systems (*e.g., Hotline*)
- ✓ Review findings from Auditing & Monitoring efforts
- ✓ Internal/external benchmarking; *industry risk inventories, resources, compliance failures*
- ✓ Leverage available regulatory/enforcement agency resources, information, trends

More…

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

16

Identification of Compliance Risk – *Risk Inventory*

Top Compliance Risk Areas - *Examples*

- Antitrust/Competition Law
- Bribery & Corruption
- Discrimination/Harassment
- Health/Safety
- ESG/Environmental
- Privacy/Data Protection
- Insider Trading
- Social Media Risk
- Mergers & Acquisitions
- Conflicts of Interest/Gifts
- Government Contracts
- Trade Compliance
- Financial Accounting
- Records Management
- Cyber Security/Threats
- Intellectual Property
- Third-Parties/Agents
- Money Laundering

17

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

17

Identification of Compliance Risk – *Connecting Compliance Risk to ERM*

Key Considerations:

- ERM provides a portfolio view of the most important risks across an organization
  - Primary goal is evaluating risks for purposes of considering business objectives, creating value, and making strategy decisions
- Compliance Risk Management focuses specifically on compliance and compliance-related risks
  - Ongoing effort to minimize risk and liabilities associated with compliance failures and wrongdoing
- ERM portfolio view enables organizations to effectively consider relationships/interactions of various risks on each other
  - Allows for better decision-making, risk response, and resource allocation; *important when considering compliance risk*

18

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

18

Identification of Compliance Risk – *Connecting Compliance Risk to ERM*

Key Considerations (*Cont.*):

- Top compliance risks should be included in the ERM portfolio view, but not all compliance risks will be identified as priorities
  - Some compliance risks may be a lower priority when viewed against other risks at the enterprise level
- Regardless of ERM risk priorities at the enterprise level, C&E Programs have an ongoing responsibility to manage/mitigate all important compliance risks facing the organization
  - Maintain a Compliance Risk Inventory and continually assess and prioritize top risks for management and mitigation
- Important for CCO's to stay engaged and connected with leadership, business leaders, Internal Audit, ERM, and other risk functions to provide ongoing input and partnership regarding compliance risks related to business strategy and objectives

Effects of Intentional *vs.* Unintentional Risk Events

Risk Identification – *Effects of Intentional vs. Unintentional Risk Events*

Defined and Distinguished

- **Intentional vs. Unintentional Risk Events – *Compliance-Related***
  - ***Intentional*** - Risks events that generally arise from overt and intentional acts intended to cause harm and/or efforts to engage in wrongdoing or criminal conduct.
    - *Examples: Fraud, corruption, bribery, hacking, conflicts of interest, theft, internal/external data breaches, etc.*
  - ***Unintentional*** - Risk events that typically arise from negligence, carelessness, mistakes, lack of training or experience, and other innocent causes.
    - *Examples: Accounting errors, equipment misuse resulting in injury, new regulations, network failures, unknowns…*
  - Both can result in reputational damage and create liability. Intentional risk events cause greater liability when organizations are faced with enforcement challenges as a result of wrongdoing
  - Effective and timely identification and response to compliance risk events will help to minimize liability and other harm to the organization caused by the event.

Risk Identification – *Scenario #2*

Risk Identification - *Scenario #2*

You have just been hired as the first E&C Risk Officer for a large, global pharma company. Over the last 5 years, the company has acquired 25 smaller firms around the world, but given other business priorities, has allowed them to maintain their existing C&E infrastructures and RM programs until resources and budgets are available to fully integrate them into the parent.

In addition, to help minimize the financial impact of your new position and budget, the company decides to raise the cost of its popular, life-saving cancer drug by 5000%.

What immediate questions would you have, and what potential risks and considerations come to mind?

Risk Identification - *Scenario #2*

Questions, Risks, and Considerations – *Discussion*

Risk Identification – *Key Takeaways*

25

Risk Identification – *Key Takeaways*

Practice Takeaways

- ✓ Ongoing support, collaboration, and input from management and leadership is essential for effective practice.
- ✓ An organization's risk universe is dynamic, evolving, and requires continued monitoring, management, and updates
- ✓ Assure meaningful and effective processes and methodologies are in place to identify and document risks relevant to the organization
- ✓ High-level prioritization of risks from Risk Inventory helps to inform Risk Assessment focus on the most important risks facing the organization
- ✓ Leverage Risk Inventory to maintain a listing of *all* compliance risks facing the organization, to include lower level risks for action; *continuously monitor and re-prioritize as needed*
- ✓ Collaborate and partner with other risk leaders and functions in the organization to support ongoing effectiveness

26

Appendix

27

Risk Identification - *Scenario #1 Discussion*

Key Risks and Issues

- ESG risks and liabilities
- Third-Party management/relationship risks
- Trade Compliance risks
- EPA violations and other related enforcement challenges
- Potential labor violations (*child, forced, etc.*)
- Antitrust/Competition law
- Reputational risk
- *Other*

Considerations

- Potential environmental and labor risks/issues; significant reputational damage to the organization, to include substantial civil and criminal liabilities. An immediate audit and assessment of the relationship, vendor operations, and vendor business practices is warranted to determine appropriate next steps (*relationship/contract termination, potential disclosures of any wrongdoing, etc.*).

28

Risk Identification - *Scenario #2 Discussion*

Key Questions

- Did M&A Due Diligence efforts include C&E risk? Did C&E function provide input?
- Were any known C&E issues and/or risks identified? Have they been addressed?
- Is the company notified when C&E issues/risks arise and how does it respond?
- How does the company monitor C&E risk in the acquired entities?
- What is the rationale for delaying integration efforts?
- Has a strategic plan been established to integrate the firms (*including timing, budget, resources*)?

Considerations

- Assumption/ownership of risk liabilities; cultural challenges; business priorities over C&E; lack of monitoring/oversight of C&E risk; no centralized/consistent C&E standards, expectations, and RM infrastructures; risk exposure in areas such as corruption/bribery, legal/regulatory compliance, culture, trade compliance, among others; parent company not meeting C&E program/RM expectations for effectiveness; and significant reputational damage from drug price increase.

Compliance Risk Management – *Introduction/Overview*

NEXT SESSION – *RISK APPETITE AND TOLERANCE*

60 MINUTE BREAK