COMPLETING THE COMPLIANCE RISK MANAGEMENT CYCLE

Caroline McMichen

1

Completing the Compliance Risk Management Cycle

In this session, we will discuss the five elements of ERM as defined by COSO and discuss their application to C&E programs:

- Governance and Culture
- Strategy and Objective-Setting
- Performance
- Review and Revision
- Information, Communication and Reporting

2

COSO ERM Principles

- Source: COSO, *Enterprise Risk Management – Integrating with Strategy and Performance* (June 2017)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

3

Elements of Compliance & Ethics Programs

1. Standards and procedures
2. Governance, oversight, and authority
3. Due diligence in delegation of authority
4. Communication and training
5. Monitoring, auditing, and reporting systems
6. Incentives and enforcement
7. Response to wrongdoing
8. Risk assessment
9. Continuous program improvement

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

4

Relationship to Compliance & Ethics Programs

- Elements of an effective compliance and ethics program already share numerous characteristics with the COSO ERM and IC frameworks most notably:
  - A focus on, and a process for, identifying and assessing risk
  - Development of a governance structure, policies and procedures
  - Importance of culture
  - Value placed on communications and reporting
  - An expectation of continuous improvement in the program

Polling Question

How is compliance risk assessed in your organization?

- As part of the organization's ERM assessment
- Compliance does its own assessment of compliance risk
- Internal audit assess compliance risk as part of it risk assessment
- ERM, Compliance and IA each do an assessment of compliance risk
- Not sure

COSO ERM Principles

- Source: COSO, *Enterprise Risk Management – Integrating with Strategy and Performance* (June 2017)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

7

COSO ERM Principles Applied to C&E Programs

Governance & Culture

➢ **Require the Board/Committee to oversee compliance risk management and the C&E program**

- Document in Board and/or Committee Charter
- Include a member who has compliance expertise
- Ensure independence of CCO and C&E function -Who does the CCO report to? How are they hired, fired, evaluated? CCO has direct access to, and regularly communicates with the Board/Committee
- Grant sufficient authority to the CCO
- Ensure sufficient staffing and resources are provided for an effective C&E program

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

8

Governance & Culture

COSO ERM Principles Applied to C&E Programs

- **Ensure the Board/Committee is knowledgeable of, and demonstrates oversight of, the C&E program**
  - Allow for appropriate frequency and time allocated for discussion
  - Executive sessions are regularly held with CCO and key compliance stakeholders
  - Content of CCO reports is comprehensive, including compliance risk assessment, significant investigations and remediation efforts
  - Discussion and decisions are documented in minutes
  - Establish policies, procedures and escalation protocols related to the operation of the C&E program

(Continued…)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Governance & Culture

COSO ERM Principles Applied to C&E Programs

- **Ensure the Board/Committee is knowledgeable of, and demonstrates oversight of, the C&E program**
  - Board/Committee is knowledgeable of key compliance policies, and approves the Code of Conduct
  - Board/Committee members receive training as needed on significant compliance risk areas facing the organization and, on their role and responsibilities as they pertain to the C&E program

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Governance & Culture

COSO ERM Principles Applied to C&E Programs

- **Board and Leadership demonstrate commitment to core values and a culture of risk awareness, compliance and ethics**
  - Regularly communicate about organizational values, expectations and importance of compliance and ethics
  - Include accountability for management of compliance risks and compliance program implementation in job descriptions, performance evaluation and incentive programs
  - Promote organizational justice, including accountability for wrongdoing, fairness and consistency in discipline, and fairness in promotions
  - Take all allegations seriously and have zero tolerance for retaliation
  - Perform ongoing monitoring of organizational culture

(Continued…)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

11

11

Governance & Culture

COSO ERM Principles Applied to C&E Programs

- **Board and Leadership demonstrate commitment to core values and a culture of risk awareness, compliance and ethics**
  - Communicate lessons learned from compliance and ethics failures
  - Hire a CCO and compliance team staff with appropriate experience, expertise and resources
  - CCO is a respected member of the senior leadership team and participates in business strategy and planning sessions
  - Establish an internal cross-functional compliance and ethics committee
  - Perform background checks aimed at screening for compliance risk appropriate for the position
  - Perform risk-based due diligence on third parties

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

12

12

Governance & Culture

COSO ERM Principles Applied to C&E Programs

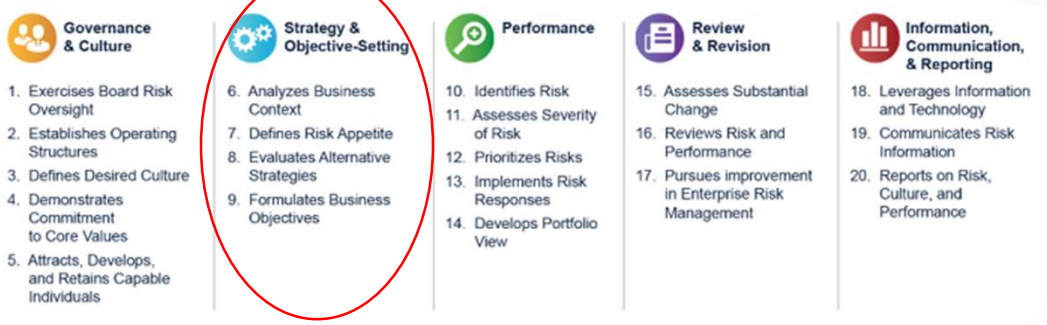
- **Establish a Code of Conduct and C&E policies that promote a culture of compliance and ethics**
  - Align with the organization's vision, mission and values
  - Set behavioral expectations, including speaking up
  - Address all relevant compliance risk areas
  - Provide communication and training on the Code and compliance risk areas that is tailored to the role and includes guidance on ethical decision-making

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

13

COSO ERM Principles



- Source: COSO, *Enterprise Risk Management – Integrating with Strategy and Performance* (June 2017)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

14

Strategy & Objective-Setting

COSO ERM Principles Applied to C&E Programs

- **Consider compliance and ethics risks in business strategy and objectives**
  - Ensure CCO participation in business strategy discussions
  - How might C&E risks be affected by internal factors such as changes in people, structures, processes, technology etc.?
  - How might C&E risks be affected by external factors such as competitive, economic, enforcement trends or regional/local legal frameworks?
  - Evaluate the relationships between compliance risks and the achievement of business objectives
  - Consider interactions between compliance risks and other risks when developing objectives

(Continued…)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Strategy & Objective-Setting

COSO ERM Principles Applied to C&E Programs

- **Consider compliance and ethics risks in business strategy and objectives**
  - Consider impact of strategic decisions on the C&E program and procedures (ex. – mergers and acquisitions)
  - Incorporate C&E risk remediation requirements in business case when evaluating the cost-benefit of a particular strategy or objective
  - Incorporate compliance risk management and accountability (including effectiveness of C&E program implementation) into performance measures and related evaluations

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Strategy & Objective-Setting

COSO ERM Principles Applied to C&E Programs

- **Establish and apply organizational risk appetite**
  - Identify and evaluate compliance risks associated with business objectives
  - Consider compliance risk by type of risk, business unit or function, and location
  - Develop specific compliance risk appetite statements in support of overall risk appetite
  - Develop tolerances for specific risk areas
  - Apply compliance risk appetite and tolerances when performing monitoring or auditing activities
  - Discuss risk appetite with key stakeholders on a regular basis and update as necessary

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

17

COSO ERM Principles

- Source: COSO, *Enterprise Risk Management – Integrating with Strategy and Performance* (June 2017)

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

18

Performance

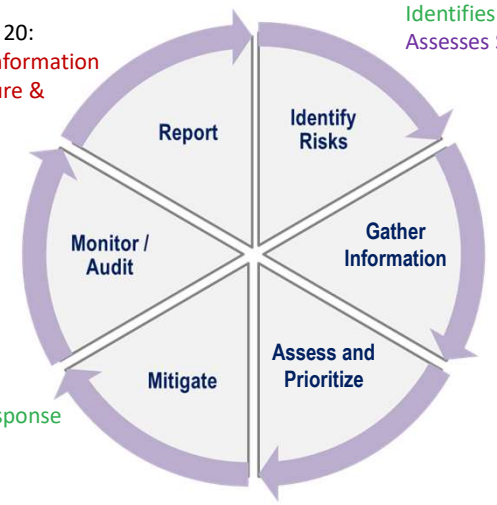
Review & Revision

Information, Communication, & Reporting

COSO ERM Principles Applied to C&E Programs

ERM Principle #10 & 15:
Identifies Risk
Assesses Substantial Change

ERM Principles #19 & 20:
Communicates Risk Information
Reports on Risk, Culture & Performance



ERM Principle #18:
Leverages Information & Technology

ERM Principles #16 & 18:
Reviews Risk and Performance
Leverages Info & Technology

ERM Principle #13:
Implements Risk Response

ERM Principles #11 & #12:
Assesses Severity of Risk
Prioritizes Risk

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

19

19

Performance

Review & Revision

Information, Communication, & Reporting

COSO ERM Principles Applied to C&E Programs

Additionally, these principles are applied throughout the entire compliance risk management cycle:

➢Develops Portfolio View

- Integrate compliance risk management with ERM
- Consider risk and risk response interactions
- Have regular discussions about compliance risk with business

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

20

20

Performance

Review & Revision

COSO ERM Principles Applied to C&E Programs

Information, Communication, & Reporting

Additionally, these principles are applied throughout the entire compliance risk management cycle:

➢Pursues improvement in ERM

- Continuously improve compliance risk management programs and processes
- Maintain awareness of current trends and best practices in compliance risk management
- Obtain feedback from the Board and Leadership on the quality and usefulness of compliance risk information shared
- Evaluate the effectiveness of the compliance risk management process and overall C&E program periodically by self-assessment, benchmarking or independent third-party review.

21

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

21

Performance

Review & Revision

COSO ERM Principles Applied to C&E Programs

Information, Communication, & Reporting

Additionally, these principles are applied throughout the entire compliance risk management cycle:

➢Communicates risk information

- Ensure employees receive clear and regular communication and training on their roles regarding C&E and compliance risk management
- Establish protocols for escalation

➢Leverages information and technology

- Utilize technology to deliver training, facilitate risk assessment and risk management processes

➢Reports on risk, culture and performance

- Provide periodic reports on meaningful C&E program metrics, investigations and significant remediation efforts

22

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

22