Application of the COSO ERM Framework to Compliance Risk Management

Urton Anderson
Daniel Roach
Paul Sobel
Gerry Zack

1

1

Today's Objectives

- Learning Objectives:
  - Apply the COSO Enterprise Risk Management framework to the management of compliance risk
  - Map the elements of an effective compliance and ethics program to ERM
  - Understand how to apply the recently-published guidance from COSO authored by SCCE

2

2

AU1

Polling Question

Which best describes your role in your organization:

- Internal audit
- Compliance
- Risk management
- Other

3

3

The Committee of Sponsoring Organizations (COSO) is a joint initiative established in 1985 to sponsor the National Commission on Fraudulent Financial Reporting.

American Accounting Association – Thought Leaders in Accounting	7,000
AICPA American Institute of CPAs	430,000
fei Financial Executives International	10,000
ima The Association of Accountants and Financial Professionals in Business	125,000
The Institute of Internal Auditors	210,000

> 780,000 members

4

4

COSO's Mission & Vision

COSO's **Mission** is "To help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence."

COSO's **Vision** is "To be globally recognized as an authority on internal controls and a thought leader on risk management, governance and fraud deterrence."

5

5

History of Framework Development

- 1992 – Internal Control – Integrated Framework (ICIF)
- 2004 – Enterprise Risk Management (ERM) – Integrated Framework
- 2013 – ICIF Updated Framework
- 2017 – ERM Updated Framework

6

6

COSO ERM Graphic

- Consists of five components, supported by 20 principles
- Source – COSO, *Enterprise Risk Management – Integrating with Strategy and Performance* (June 2017)

7

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

7

COSO ERM Principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

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

8

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

8

COSO ERM – Key Definitions

- **Enterprise Risk Management** – The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value.
- **Risk** – The possibility that events will occur and affect the achievement of strategy and business objectives
- **Severity** – A measurement of considerations such as the likelihood and impact of events or the time it takes to recover from events

9

9

COSO ERM
The Role of Risk in Strategy Setting

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

10

10

Polling Question

Does your organization utilize the COSO Framework for Enterprise Risk Management in the management of risk?

- Yes
- No
- Not sure

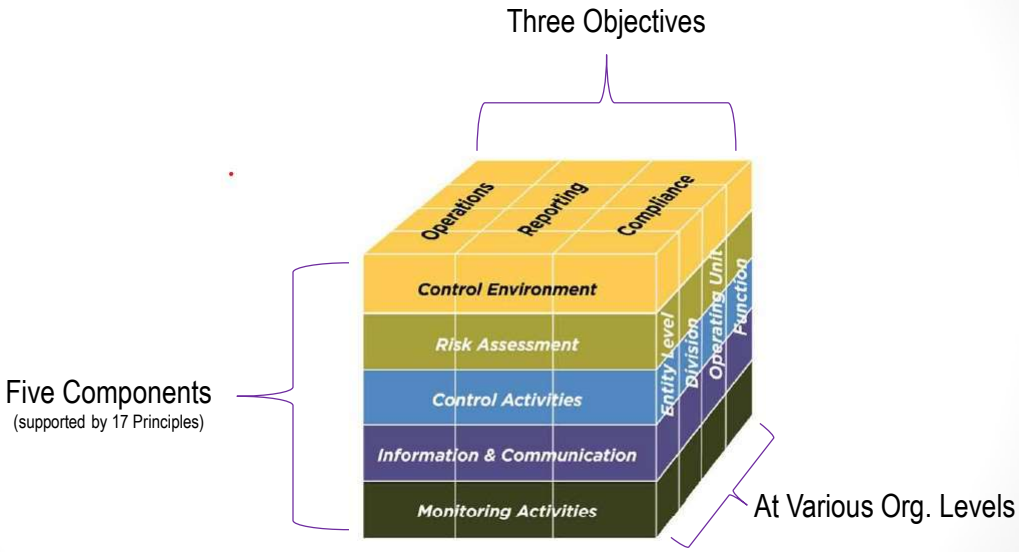
11

Internal Control

- Defined by COSO as:
  - A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance

12

COSO Internal Control Framework (2013)



SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

13

Relationship to *The IIA's Three Lines Model* (2020)

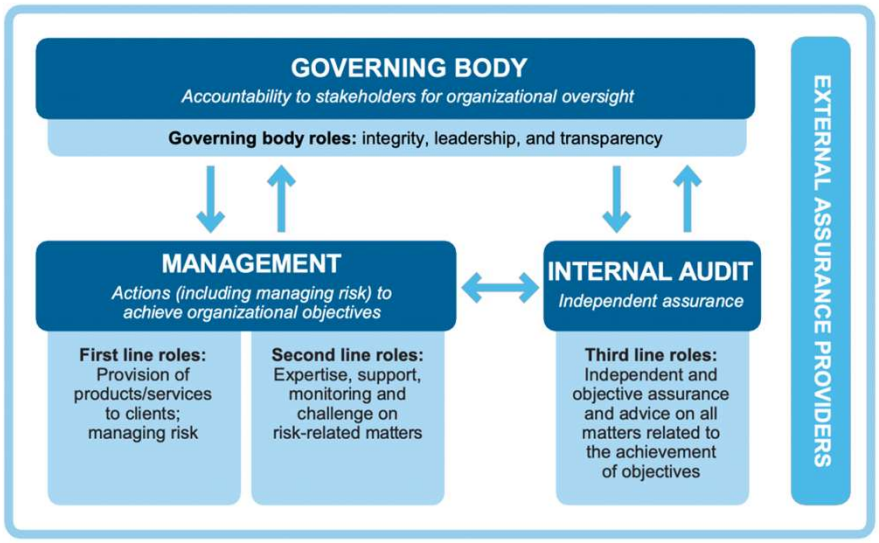
- Formerly the "Three Lines of Defense" model, until 2020 revision
- Assists in identifying structures and processes that ensure the achievement of objectives and facilitate strong governance and risk management
  - Governing body
  - Management
  - Internal audit
  - External assurance
- Permits CCO (or CRO) to have a direct reporting line to the governing body (similar to Internal Audit)
- Identifies compliance-related responsibilities at:
  - Governing body
  - 1st line roles
  - 2nd line roles

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

14

The IIA's Three Lines Model



- Source: *The IIA's Three Lines Model*

15

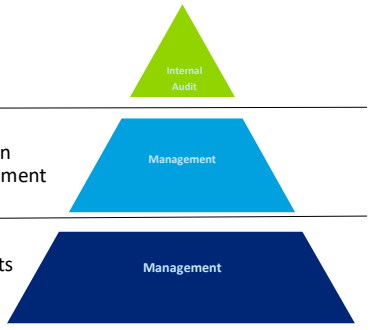
15

The IIA's Three Lines Model

"The Third Line"
Independent assurance and advice.

"The Second Line"
Expertise, support, monitoring and challenge to assist in managing risk; Development, implementation and improvement of risk management practices; Analysis and reporting.

"The First Line"
Management of risk in connection with providing products and services to clients; Establishing and maintaining internal controls to ensure compliance.



16

16

Polling Question

AU4

Does your organization use the COSO Internal Control Framework and/or the "Three Lines Model"?

- COSO Internal Control and Three Lines Model
- COSO Internal Control only
- Three Lines only
- Neither
- Not sure

17

17

Relationship to Compliance & Ethics Programs

- Elements of an effective compliance and ethics program already share numerous characteristics with the ERM and IC frameworks, and the Three Lines Model, 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

18

18

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

19

19

15 Minute Break

20

20

GOVERNANCE & CULTURE

1. Exercises board risk oversight
2. Establishes operating structures
3. Defines desired culture
4. Demonstrates commitment to core values
5. Attracts, develops, and retains capable individuals

21

21

1. Exercises Board Risk Oversight

<u>COSO ERM Considerations:</u>

- Accountability and responsibility
- Skills, experience, and business knowledge
- Independence
- Suitability of ERM
- Understand organizational bias

22

22

ERM Principle 1 Applied to C&E Programs

Table 2.1: Exercises board risk oversight

KEY CHARACTERISTICS:
■ Require the board to oversee compliance risk management and the C&E program, including the approval of its charter
■ Ensure that the board is knowledgeable of and demonstrates oversight of the C&E program (regular part of agendas, monitors compliance metrics, holds regular executive sessions with CCO and others)
■ Require that the board includes a member who possesses compliance expertise
■ Document evidence of board oversight of the C&E program in minutes
■ Provide input or approve appointment/dismissal/reassignment of CCO and ensures independence
■ Ensure that sufficient resources are provided for the C&E program
■ Receive regular reports from the CCO
■ Ensure the board is informed about material investigations and remediation efforts and provides input

2. Establishes Operating Structures

<u>COSO ERM Considerations:</u>

- Operating structure and reporting lines
- ERM structures
  - Committees
- Authority and responsibilities
- ERM within the evolving entity
  - Tailored to the organization

ERM Principle 2 Applied to C&E Programs

Table 2.2: Establishes operating structures

KEY CHARACTERISTICS:
■ Maintain independence of the CCO and the compliance and ethics function
■ Ensure the CCO directly reports to and regularly communicates with the board
■ Ensure that the CCO and C&E program have high stature relative to other functional leaders
■ Grant sufficient authority to the CCO to manage the program effectively
■ Provide sufficient resources for the C&E program to be effective
■ Address C&E program oversight in the charter (including delegation to a designated committee, if applicable)
■ Document policies and procedures specific to the operation of the C&E program
■ Establish protocol/procedures for escalation of significant compliance risk events

25

25

3. Defines Desired Culture

COSO ERM Considerations:

- Culture and desired behaviors
- Applying judgment
- Effect of culture
- Aligning core values, decision-making, and behaviors
- Shifting culture

26

26

ERM Principle 3 Applied to C&E Programs

Table 2.3: Defines desired culture

KEY CHARACTERISTICS:
■ Ensure the board is knowledgeable of and approves a code of conduct/ethics and other key compliance policies
■ Explain expectations relating to ethics and compliance in a code of conduct/ethics
■ Provide and require training on the code of conduct and on ethical decision-making for all staff (including board members)
■ Perform ongoing monitoring or assessment of organizational culture
■ Develop objectively measurable compliance metrics tied to performance evaluations and compensation, where appropriate
■ Adopt meaningful incentives to promote consistent execution of the C&E program
■ Include references to organizational values, expectations, and importance of ethics in communications from leadership

27

27

4. Demonstrates Commitment to Core Values

COSO ERM Considerations:

- Reflecting core values throughout the organization
- Embracing a risk-aware culture
- Enforcing accountability
- Holding itself accountable
- Keeping communication open and free from retribution
- Responding to deviations in core values and behaviors

28

28

ERM Principle 4 Applied to C&E Programs

Table 2.4: Demonstrates a commitment to core values

KEY CHARACTERISTICS:
▪ Actively promote a culture of compliance risk awareness, including setting an ethical and compliant tone by leadership
▪ Balance business incentives with material compliance incentives
▪ Incorporate accountability for the management of (i) compliance risks and (ii) compliance program implementation into employee performance measurement, promotions, and incentive programs, particularly at senior levels
▪ Protect those who report suspected wrongdoing, with zero tolerance for retaliation
▪ Take allegations of wrongdoing seriously and investigate in a timely manner
▪ Promote organizational justice, including accountability for wrongdoing, fairness and consistency in discipline, and fairness in promotions
▪ Communicate lessons learned from compliance and ethics failures across the organization in appropriate detail

29

5. Attracts, Develops, and Retains Capable Individuals

<u>COSO ERM Considerations:</u>

- Establishing and evaluating competence
- Attracting, developing, and retaining individuals
- Rewarding performance
- Addressing pressure
- Preparing for succession

30

ERM Principle 5
Applied to C&E Programs

Table 2.5: Attracts, develops, and retains capable individuals

KEY CHARACTERISTICS:
■ Hire and retain a CCO with appropriate experience/expertise to lead the C&E program
■ Staff the compliance team with individuals that possess relevant expertise
■ Perform background checks aimed at screening for compliance risk, tailored to the level of risk associated with each position
■ Consider employee execution of and adherence to the requirements and expectations of the C&E program in the preparation of performance evaluations
■ Appropriately tailor compliance training based on the compliance risks encountered for specific roles in the organization
■ Perform risk-based due diligence on third parties

31

31

STRATEGY & OBJECTIVE-SETTING

6. Analyzes business context
7. Defines risk appetite
8. Evaluates alternative strategies
9. Formulates business objectives

32

32

6. Analyzes Business Context

COSO ERM Considerations:

- Understanding business context
- Considering external environment and stakeholders
- Considering internal environment and stakeholders
- How business context affects risk profile

33

33

ERM Principle 6
Applied to C&E Programs

Table 3.1: Analyzes business context

KEY CHARACTERISTICS:
■ Consider and reflect organizational strategy in performing compliance risk assessments and managing compliance risk
■ Consider how compliance risks are affected by internal changes, such as changes in people, structures, processes, technology, etc.
■ Evaluate effects of external factors (e.g., competitive, economic, enforcement trends, environmental, political, social forces) on compliance risks
■ Identify and consider risk interdependencies in the development of strategy
■ Give consideration to cultural and regional differences in legal frameworks based on locations where the organization operates

34

34

7. Defines Risk Appetite

COSO ERM Considerations:

- Applying risk appetite
- Determining risk appetite
- Articulating risk appetite
- Using risk appetite

Key Definitions:

- **Risk** – The possibility that events will occur and affect the achievement of strategy and business objectives
- **Risk Appetite** – The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value
- **Tolerance** – The boundaries of acceptable variation in performance related to achieving business objectives

35

35

ERM Principle 7 Applied to C&E Programs

Table 3.2: Defines risk appetite

KEY CHARACTERISTICS:
■ Consider compliance risk as part of the organization's risk profile in determining risk appetite
■ Consider compliance risk by (i) type of risk (e.g., anti-bribery), (ii) business unit or organizational function (e.g., human resources), and (iii) location or region
■ Determine and evaluate the relationships between compliance risks and the achievement of business objectives
■ Discuss risk appetite on a regular basis and update as necessary based on changes in compliance risk
■ Consider developing specific risk-centric appetite statements associated with compliance risks in support of organizational risk appetite and tolerance

36

36

8. Evaluates Alternative Strategies

COSO ERM Considerations:

- Aligning strategy with core values and risk appetite
- Understanding the implications from chosen strategy
- Making changes to strategy
- Mitigating bias when evaluating alternative strategies

37

37

ERM Principle 8 Applied to C&E Programs

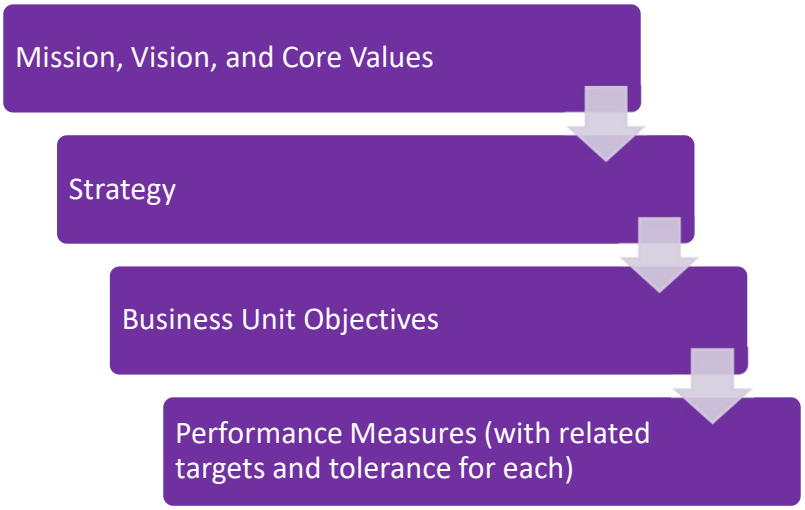
Table 3.3: Evaluates alternative strategies

KEY CHARACTERISTICS:
■ Ensure that the CCO has a seat at the table in discussions of strategies
■ Solicit input and insight from the CCO regarding how strategy affects compliance risk
■ Perform risk-based due diligence on merger and acquisition targets prior to execution of the transaction
■ Consider implications of strategic decisions (including subsequent changes in strategy) in the design of the C&E program

38

38

9. Formulates Busines Objectives



Adapted from *Risk Appetite – Critical to Success: Using Risk Appetite to Thrive in a Changing World*, COSO, May 2020

39

39

9. Formulates Business Objectives

COSO ERM Considerations:

- Establishing business objectives
- Aligning business objectives with strategy
- Understanding the implications from chosen business objectives
- Categorizing business objectives
- Setting performance measures and targets
- Understanding tolerance
- Performance measures and established tolerance

40

40

ERM Principle 9 Applied to C&E Programs

Table 3.4: Formulates business objectives

KEY CHARACTERISTICS:
■ Identify and evaluate compliance risks associated with planned business objectives
■ Consider establishing compliance as a separate business objective
■ Incorporate compliance risk management and accountability into performance measures and related evaluations
■ Consider interactions between compliance and other risks based on changes in business objectives
■ Include objectively measured compliance metrics within business objectives, reflecting the management of compliance risk and the effectiveness of C&E program implementation, and carry appropriate weight in incentive and other compensation decisions

41

41

15 Minute Break

42

42

PERFORMANCE

10. Identifies risk
11. Assesses severity of risk
12. Prioritizes risk
13. Implements risk responses
14. Develops portfolio view

43

10. Identifies Risk

<u>COSO ERM Considerations:</u>

- Identifying risk
- Using a risk inventory
- Approaches to identifying risk
- Framing risk

44

Identifying Risk

Figure 4.1

APPROACHES FOR IDENTIFYING RISKS*						
Types of Risk	Cognitive Computing	Data Tracking	Interviews	Key Indicators	Process Analysis	Workshops
Existing	✓	✓	✓	✓	✓	✓
New	✓	✓			✓	✓
Emerging	✓		✓	✓		✓

*COSO, *Enterprise Risk Management: Integrating with Strategy and Performance*, Volume 1, p. 69

45

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

45

Polling Question

Does your organization use data tracking and cognitive computing to assess risk?

- Data Tracking
- Cognitive Computing
- Both Data Tracking and Cognitive Computing
- Organization does not do a risk assessment
- Not sure

46

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

46

ERM Principle 10 Applied to C&E Programs

Table 4.1: Identifies risk

KEY CHARACTERISTICS:
■ Describe the compliance risk identification and assessment process in documented policies and procedures
■ Identify compliance risks associated with planned strategy and business objectives
■ Assess internal and external environments to identify risks
■ Create process for identifying new and emerging risks
■ Consider risks associated with use of third parties
■ Consider information gathered through hotlines, other reporting channels, and results of investigations

47

47

Figure 4.2

LIKELIHOOD OF OCCURENCE*		
Scale	**Existing Controls**	**Frequency of Noncompliance**
5 Almost Certain	■ No controls in place ■ No policies or procedures, no responsible person(s) identified, no training, no management review	Expected to occur in most circumstances More than once per year
4 Likely	■ Policies and procedures in place but neither mandated nor updated regularly ■ Controls not tested or tested with unsatisfactory results ■ Responsible person(s) identified ■ Some formal and informal (on-the-job) training ■ No management reviews	Will probably occur At least once per year
3 Possible	■ Policies mandated, but not updated regularly ■ Controls tested only occasionally, with mixed results ■ Responsible person(s) identified ■ Training is provided when needed ■ Occasional management reviews are performed, but not documented	Might occur at some time At least once in 5 years
2 Unlikely	■ Policies mandated and updated regularly ■ Controls tested with mostly positive results ■ Regular training provided to the identified responsible person(s), but not documented ■ Regular management reviews are performed, but not documented	Could occur at some time At least once in 10 years
1 Rare	■ Policies mandated and updated regularly ■ Controls regularly tested with positive results ■ Regular mandatory training is provided to the identified responsible person(s), and the training is documented ■ Regular management reviews are performed and documented	May only occur in exceptional circumstances Less than once in 10 years

*Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 30, https://compliancecosmos.org/compliance-risk-assessments-introduction.

48

48

Figure 4.3

IMPACT OF COMPLIANCE RISKS

Scale	Legal*	Financial#	Operational (Potential Disruption)*	Reputation (Image)+	Health and Safety*	Ability to Pursue Strategic Goals*
1 Insignificant	In compliance	< $1 million	< 1/2 day	No press exposure	No injuries	Little or no impact
2 Minor	Civil violation with little/no fines	$1–$5 million	< 1 day	Localized negative impact on reputation (such as a single large customer) but recoverable	First aid treatment	Minor impact
3 Serious	Significant civil fines/penalties	$5–$25 million	1 day–1 week	Negative media coverage in a specific U.S. region or a foreign country	Medical treatment	Major impact
4 Disastrous	Serious violation, criminal prosecution probable	$25–$100 million	1 week–1 month	Negative U.S. national or international media coverage (not front page)	Death or extensive injuries	Significant impact
5 Catastrophic	Significant violation, criminal conviction probable, loss of accreditation or licensure	> $100 million	> 1 month	Sustained U.S. national (and international) negative media coverage (front page of business section)	Multiple deaths or several permanent disabilities	Loss of accreditation or license

Amounts are examples only; each organization should set amounts to reflect its size and financial strength.

*Adapted from Judith W. Spain, *Compliance Risk Assessments: An Introduction* (Minneapolis: Society of Corporate Compliance and Ethics, 2020), 39, https://compliancecosmos.org/compliance-risk-assessments-introduction

+ Adapted from Deloitte, *Compliance risk assessments: The third ingredient in a world-class ethics and compliance program*, Deloitte Development LLC, 2015.

11. Assesses Severity of Risk

COSO ERM Considerations:

- Assessing severity at different levels of the entity
- Selecting severity measures
  - Qualitative
  - Quantitative
  - Frequency
- Assessment approaches
  - Probabilistic approaches
  - Non-probabilistic approaches
- Inherent, target, and residual risk
- Depicting assessment results
- Identifying triggers for reassessment
- Mitigating effects of bias in assessments

11. Assesses Severity of Risk

COSO Definitions:

- **Inherent Risk** – The risk to an entity in the absence of any direct or focused actions by management to alter its severity
- **Target Residual Risk** – The amount of risk that an entity prefers to assume in the pursuit of its strategy and business objectives, knowing that management will implement, or has implemented, direct or focused actions to alter the severity of the risk
- **Actual Residual Risk** – The risk remaining after management has taken action to alter its severity

51

51

ERM Principle 11 Applied to C&E Programs

Table 4.2: Assesses severity of risk

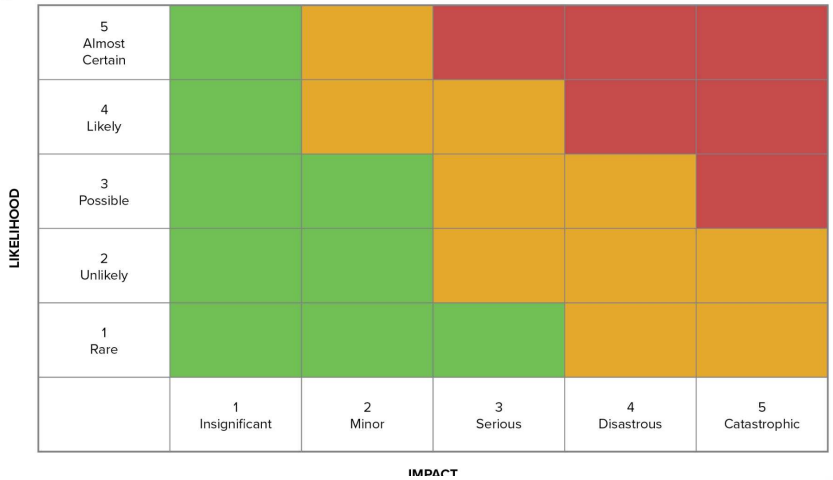
KEY CHARACTERISTICS:
■ Adopt a uniform scale/scoring system for measuring severity of compliance risks
■ Consider qualitative and quantitative measures
■ Establish criteria to assess impact and likelihood of compliance risk event occurrence
■ Assess severity of risk at different levels (organizational, regional, affiliate, etc.)
■ Consider design and operation of internal controls designed to prevent or detect compliance risk events
■ Minimize bias and inadequate knowledge in assessing severity (e.g., minimize self-assessments, use multidisciplinary teams)

52

52

Depicting Assessment Results

Figure 4.4



53

53

12. Prioritizes Risks

COSO ERM Considerations:

- Establishing the criteria
- Prioritizing risk
- Using risk appetite to prioritize risks
- Prioritization at all levels

54

54

ERM Principle 12 Applied to C&E Programs

Table 4.3: Prioritizes risks

KEY CHARACTERISTICS:
■ Prioritize compliance risks based on assessed level of risk relative to meeting of business objectives
■ Use objective scoring based on assessment
■ Consider use of other assessment criteria (trend, velocity, etc.) in prioritizing compliance risks
■ Consider possible effects of planned changes in strategy and operations
■ Develop risk-based action plans for mitigation (risk responses, implemented in next step)

55

55

13. Implements Risk Responses

<u>COSO ERM Considerations:</u>

- Choosing risk responses
  - Accept
  - Avoid
  - Pursue
  - Reduce
  - Share
- Selecting and deploying risk responses
- Considering costs and benefits of risk responses

56

56

ERM Principle 13 Applied to C&E Programs

Table 4.4: Implements risk responses

KEY CHARACTERISTICS:
■ Consider potential need for modifications in each element of the C&E program when designing risk responses
■ Design compliance risk responses that consider the impact on other (non-compliance) risks and risk responses
■ Assign accountability for each compliance risk response (including timeline, etc.)
■ Follow up to determine whether compliance risk responses have been properly implemented as designed
■ Consider compliance risk responses when developing monitoring and auditing plans

57

57

14. Develops Portfolio View

COSO ERM Considerations:

- Understanding a portfolio view
- Developing a portfolio view
- Analyzing the portfolio view

58

58

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

59

59

ERM Principle 14 Applied to C&E Programs

Table 4.5: Develops portfolio view

KEY CHARACTERISTICS:
■ Consider risk interactions (i.e., how mitigating a compliance risk can affect other risks)
■ Consider interactions of compliance risk responses with other risk responses
■ Integrate compliance risk management with ERM
■ Have regular meetings/communications between compliance and business units

60

60

15 Minute Break

61

REVIEW & REVISION

15. Assesses substantial change
16. Reviews risk and performance
17. Pursues improvement in enterprise risk management

62

15. Assess Substantial Change

COSO ERM Considerations:

- Integrating reviews into business practices
- Internal environment
- External environment

63

ERM Principle 15 Applied to C&E Programs

Table 5.1: Assesses substantial change

KEY CHARACTERISTICS:
■ Identify drivers of change in compliance risk—internal and external
■ Consider how implementation of new strategic initiatives affects compliance risk
■ Consider how changes in senior personnel impact compliance risk and/or risk tolerance
■ Evaluate changes in laws and regulations
■ Consider developments in enforcement, guidance from regulators, and other trends
■ Assess changes in local/regional environments

64

Example Application of IIA's Three Lines Model

Figure 5.1

	1st Line	2nd Line	3rd Line
Risk Area	**Management**	**Management**	**Internal Audit**
As Identified During Risk Assessment	Structures and policies	Monitoring and support	Independent auditing
Conflict of Interest	■ Establish COI policies and procedures ■ Educate personnel about COI policies ■ Report non-compliance to COI Manager ■ Report unauthorized vendors representatives and displays ■ Advise personnel to contact Compliance with questions ■ Review annual COI disclosures	■ Annual COI disclosure ■ Purchasing and Pharmacy vendor registrations ■ Open Payments database ■ Research conflict database cross-check	■ Audit 10% of outside travel payments against Accounts Payable travel reimbursements ■ Level 2 review of COI dsclosures ■ Audit 10% of "nothing to disclose" ■ "For cause" investigations

65

16. Reviews Risk and Performance

COSO ERM Considerations:

- Integrating reviews into business practices
- Considering entity capabilities

66

ERM Principle 16 Applied to C&E Programs

Table 5.2: Reviews risk and performance

KEY CHARACTERISTICS:
■ Monitor performance against compliance and ethics metrics and report at the management and board levels
■ Update compliance risk assessments on a periodic basis
■ Develop monitoring plans for high-priority risks, assign assurance responsibilities clearly across the three lines of defense, and set clear performance expectations
■ Ensure that internal audit considers compliance risk in connection with its review of entity risk and performance
■ Periodically assess the organization's culture of compliance
■ Ensure annual C&E program workplans reflect risk assessment (cross-referenced)
■ Include appropriate audit rights clauses in third-party contracts to facilitate monitoring and auditing
■ Obtain feedback from participants in compliance training, hotline reports, employee surveys, and exit interviews
■ Require that implementation of corrective action plans is an important metric monitored by management and the board
■ Perform root cause analyses for compliance risk events experienced

67

17. Pursues Improvement in ERM

<u>COSO ERM Considerations:</u>

- Pursuing improvement
  - New technology
  - Historical shortcomings
  - Organizational change
  - Risk appetite
  - Risk categories
  - Communications
  - Peer comparison
  - Rate of change

68

ERM Principle 17
Applied to C&E Programs

Table 5.3: Pursues improvement in enterprise risk management

KEY CHARACTERISTICS:
■ Maintain awareness of current trends in compliance risk management (through training, review of regulatory guidance, etc.)
■ Ensure that compliance periodically self-assesses the C&E program's performance
■ Obtain feedback from the board on the quality and usefulness of compliance risk information shared
■ Consider obtaining periodic independent evaluation of the C&E program
■ Consider benchmarking C&E program against similar organizations
■ Review efficacy of the compliance risk assessment process on a periodic basis
■ Ensure that internal audit plays an active role in periodically evaluating the effectiveness of the C&E program

69

69

INFORMATION, COMMUNICATION & REPORTING

18. Leverages information and technology
19. Communicates risk information
20. Reports on risk, culture, and performance

70

70

18. Leverages Information and Technology

COSO ERM Considerations:

- Putting relevant information to use
- Evolving information
- Data sources
- Categorizing risk information
- Managing data
- Using technology to support information
- Changing requirements

71

71

ERM Principle 18 Applied to C&E Programs

Table 6.1: Leverages information and technology

KEY CHARACTERISTICS:
■ Ensure that compliance has access to all information relevant to effectively manage compliance risk
■ Provide compliance with relevant information technology/data analytics skills or access to such skills
■ Utilize data analytics in monitoring/auditing (monitor compliance and performance of internal controls)
■ Create automated dashboards/reports for monitoring compliance
■ Leverage technology to provide for the delivery of effective compliance and ethics training
■ Utilize technology to facilitate risk assessment process (scoring, reporting etc.)

72

72

19. Communicates Risk Information

COSO ERM Considerations:

- Communicating with stakeholders
- Communicating with the board
- Methods of communicating

73

ERM Principle 19 Applied to C&E Programs

Table 6.2: Communicates risk information

KEY CHARACTERISTICS:
■ Ensure that employees receive clear and regular communications on their roles regarding C&E
■ Require periodic reporting to the board by the CCO
■ Establish protocols and ensure a clear understanding of an escalation policy
■ Provide compliance risk communications that support and relate to training and job responsibilities
■ Engage in effective two-way communication between operations management and compliance

74

Polling Question

How is compliance risk primarily communicated to the board in your organization?

- CCO periodically meets with the board/board committee
- ERM periodically meets with the board/board committee
- IA periodically meets with the board/board committee
- Through General Counsel
- Through Executive Management
- Combination of the above
- Not sure

20. Reports on Risk, Culture, and Performance

<u>COSO ERM Considerations:</u>

- Identifying report users and their roles
- Reporting attributes
- Types of reporting
- Reporting risk to the board
- Reporting on culture
- Using key indicators
- Reporting frequency and quality

ERM Principle 20 Applied to C&E Programs

Table 6.3: Reports on risk, culture, and performance

KEY CHARACTERISTICS:
■ Provide periodic reports on compliance and ethics risk assessments and related remediation efforts tailored to key stakeholder needs
■ Develop and report on meaningful operational and substantive metrics associated with the effectiveness of the C&E program
■ Provide managers with reports on completion and results of training of their direct reports
■ Use a case management and reporting system for investigations and outcomes
■ Establish and follow a policy that clearly articulates the nature of reporting on all significant remediation efforts

77

77

15 Minute Break

78

78

WHAT DOES ALL THIS MEAN FOR THE COMPLIANCE & ETHICS PROGRAM?

79

PS1

Polling Question No. 1

Will the publication of this guidance increase the level of scrutiny placed on an organization's compliance and ethics program by Internal Audit?

- Yes
- No
- Not sure

80

Polling Question No. 2

Will the publication of this guidance increase the level of scrutiny placed on an organization's compliance and ethics program by the external auditors?

- Yes
- No
- Not sure

81

81

Polling Question No. 3

Will this guidance help organizations in meeting expectations of enforcement (e.g. DOJ) and regulators regarding compliance & ethics programs?

- Yes
- No
- Not sure

82

82

Polling Question No. 4

Will the publication of this guidance lead to a greater focus on internal controls over compliance, including the auditing and monitoring function?

- Yes
- No
- Not sure

83

83

Polling Question No. 5

Will the publication of this guidance assist in the benchmarking of compliance & ethics programs across organizations?

- Yes
- No
- Not sure

84

84

Polling Question No. 6

Which group will benefit the most from this guidance?

- Compliance professionals
- Internal auditors
- Risk professionals
- Senior management
- Members of the board of directors

85

QUESTIONS ??

86

THANK YOU !!