# SCCE COMPLIANCE & ETHICS INSTITUTE

**September 15, 2019 – National Harbor, MD**

## Effective E&C Risk Management – Part 1

***Framework, Program Essentials, and Core Practice Considerations***

**Greg Triguba, JD, CCEP, CCEP-I**
**Jim Urso, MBEC, SAFR, CCEP**

SCCE™
Society of Corporate Compliance and Ethics

1

## Workshop Agenda

I. **Ethics & Compliance Risk Management Overview**
- Value Proposition
- Risk Management Essentials: *Getting Started*
  - Defining Risk Management Practice
  - Core Program Objectives
  - Key Partnerships and Teams

II. **Risk Identification**
- Understand Organizational Risks and Define Universe
  - Top Ethics and Compliance Risk Areas; *Things that Affect Risk*
  - Defining Inherent and Control Risks
  - Internal and External Inputs
  - Management Support, Planning and Next Steps

III. **Risk Scenario #1**

2

2

## IV. Risk Assessment and Prioritization

- Primary Practice Considerations
- Legal Privilege and Risk Assessments
- Conducting a Risk Assessment
  - Key Process Steps and Considerations
  - Establish a Risk Assessment Leader
  - Select Risk Assessment Participants
- Assess Findings and Prioritize Risk
  - Risk Impact and Likelihood
  - Map Risk Assessment Findings and Prioritize
  - Management Review and Input

## V. Risk Scenario #2

3

3

## VI. Risk Management and Mitigation Strategies

- Effective Risk Management Practice
  - Risk Response: *Approach Considerations*
  - Enabling Effective Action Plans
  - Sample Risk Mitigation Actions
  - Reporting Activities

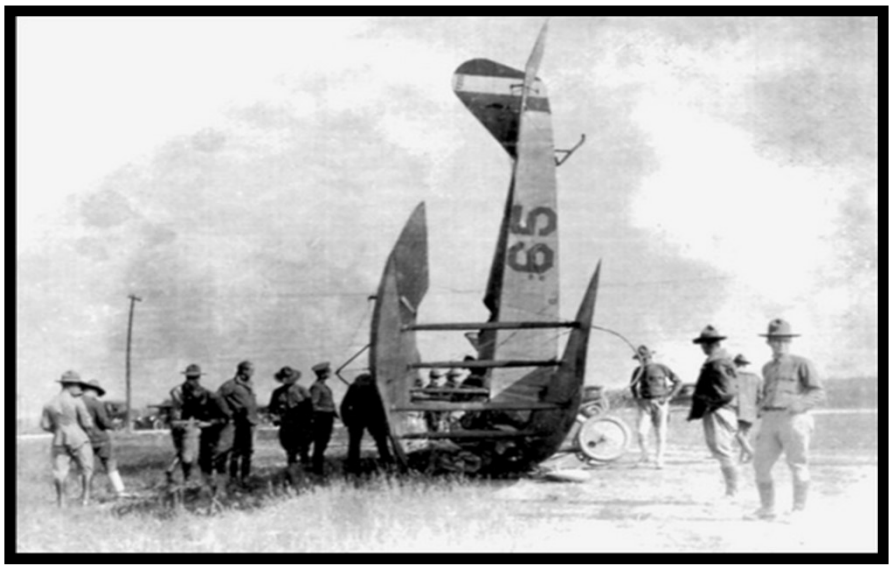
## VII. Monitoring, Auditing, and Follow-up

- Process and Management Considerations
  - Oversee, monitor and track Risk Management Plans to completion
  - Periodic auditing of Risk Management Controls
  - Subsequent Risk Assessments to ensure ongoing effectiveness
  - Ensure ongoing monitoring, auditing, and reporting activities

## VIII. Wrap-Up and Final Thoughts

4

4




5

5

# I. Ethics & Compliance Risk Management Overview

6

6

# E&C Risk Management Overview - *Value Proposition*

### *Benefits of Effective Practice:*

- Portfolio view of compliance and ethics risks; allows for effective identification, prioritization and management. Provides clarity on organizational risk appetite
- Shared-vision with leadership on top risks, resource allocation, focus and ownership; promotes dialogue and synergies among business leaders in managing risk
- Facilitates stronger change management effectiveness across the organization from a compliance and operational view
- Improves and enhances legal/regulatory compliance and risk responses both internally and externally; reduces operational losses and surprises
- Integrates and assures key ethics and compliance risks are managed and contribute to overall organizational strategy and operational objectives
- Assures the organization is working on the right stuff, at the right time, and with the right resources; protects brand, reputation and assets

7

7

# E&C Risk Management Overview - *Value Proposition*

### *Example Standards*


- **U.S. Federal Sentencing Guidelines for Organizations (USSC)**
  - *An organization "shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement [of its compliance and ethics program] to reduce the risk of criminal conduct identified through this process." (§8B2.1(c))*
  - *Risk management elements: Standards and Procedures (Internal Controls), monitoring, auditing, periodic evaluation. (§8B2.1(b)(1)(5))*
- **Sample Government Agencies recognizing importance of Risk Management**
  - DOJ, SEC, DOL, DOE, FTC
  - HHS OIG Compliance Program Guidance
  - Federal Energy Regulatory Commission (*Risk Inventory*)

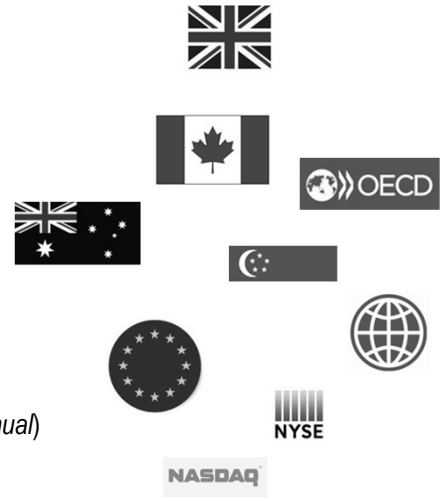
8

8

# E&C Risk Management Overview - *Value Proposition*

***Other Standards***

- EU and other International governing laws and standards
- UK Bribery Act and Foreign Corrupt Practices Act
- OECD Good Practice Guidance
- Competition Commission of Singapore
- Australian Standard – AS 3806-2006
- Competition Bureau Canada
- U.S. Sarbanes-Oxley Act of 2002
- World Bank Group Integrity Compliance Guidelines
- Stock Exchange Listing Standards (*e.g., NYSE*)
- Regulatory and legal standards unique to the business
- Enforcement officials' standards (*e.g., U.S. Attorneys' Manual*)
- COSO Internal Controls Framework




***More...***

9

9

*"The first step in the risk management process is to acknowledge the reality of risks. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning."*

Charles Tremper

**It is not about eliminating risk, but rather, taking steps to proactively and intelligently manage it!**

10

10

# Initial Step: *Risk Management Planning…*


11

11

# E&C Risk Management Overview - *Practice Essentials*

### *Defining Risk Management Practice*

| | |
|---|---|
| **Risk** | **Probability or threat of a damage, injury, liability, loss, or other negative occurrence that is caused by external or internal vulnerabilities, and that may be neutralized through preemptive action.** *BusinessDictionary.com* |
| **Risk Management** | **Identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.** *Wikipedia.org* |
| **Risk Assessment** | **Identification, evaluation, and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk.** *BusinessDictionary.com* |

### *Other Definitions?*

12

12

## E&C Risk Management Overview - *Practice Essentials*

### *Core Program Objectives:*

- Leadership and Organizational Support – *Promote positive outlook*
- Solid infrastructure, planning and implementation strategies in place
- Ensure parties involved are engaged and understand objectives
- Meaningful risk identification and scoping activities
- Effective implementation and management of Risk Assessment process to include careful documentation of findings and risk prioritization
- Enable and oversee effective risk mitigation and management plans; drive ownership and accountability throughout the business
- Monitor, Audit, Report, and Follow-up

13

13

## E&C Risk Management Overview - *Practice Essentials*

### *Key Partnerships and Teams*

- Governing Body/Senior Leadership (*Informed)*
- CECO, General Counsel, Legal/Compliance SME's
- Functional Group Partners: IT, HR, Internal Audit, Information Security, Finance, etc.
- Business/Operating Unit Representation: Leadership, management teams, regional managers, global locales, etc.
- Designated Risk Assessment Leader and team
- Consultants and other external SME's as needed

### *Other Partners?*

14

14

15

15

# II. Risk Identification

16

16

## Risk Identification – *Understand Risks and Define Universe*

***Considerations***

- Top ethics and compliance risk areas
- *Things that affect risk*
- Defining Inherent and Control Risks
- Internal and External Inputs
- Management input and support
- Planning and next steps

***What is your Risk Universe?***

17

17

## Risk Identification – *Top Ethics & Compliance Risk Areas*

- Antitrust/Competition
- Conflicts of Interest
- Corruption/Bribery
- Culture/Ethics
- Discrimination/Harassment
- Ethics & Compliance Program Infrastructure
- Environmental, Health, Safety
- Financial Accounting/Controls/Compliance
- Government Contracts/Relationships
- Intellectual Property
- Privacy/Data Protection
- Records and Information Management
- Trade Compliance (*Exports, Imports, etc.*)
- Social Media Related-Risk

18

18

# Risk Identification – *Sample Practice View*

| Legal / Regulatory Requirements | | | Business Requirements |
|---|---|---|---|
| **Industry Specific**<br>• Energy/Utilities<br>• Finance/Insurance<br>• Health Care<br>• Higher Education<br>• Industrial<br>• Manufacturing<br>• Pharmaceuticals<br>• Retail<br>• Technology<br>• Transportation<br><br>**Geography/Entity Status**<br>• Domestic<br>• International<br>• Private<br>• Public<br>• Profit<br>• Non-profit | **Antitrust/Fair Competition**<br><br>**California**<br>• Conduct business in CA?<br><br>**Consumer Protection/Product Safety**<br><br>**Corporate Governance/ Securities**<br>• Listing requirements<br>• Board matters<br>• Ethics /Whistleblower Protection<br>• Insider Trading/Reg FD<br><br>**Employment**<br>• Compensation<br>• Harassment/Discrimination<br>• Labor<br>• Leaves Administration<br>• Wage and Hour<br><br>**Environmental, Health & Safety** | **Financial**<br>• Accounting Process/Controls<br>• Financial Reporting (SEC)<br>• Tax<br><br>**Fraud and Corruption**<br>• Anti-Money Laundering<br>• Bribery (FCPA; UKBA, OECD)<br><br>**Government Relations**<br>• Fed Contractor status<br>• Working with government officials<br><br>**Information Management**<br>• Discovery/Records Retention<br>• Privacy/Data Security<br><br>**Import and Export**<br><br>**Intellectual Property**<br>• Copyright/Trademark use | **Internal Focused**<br>• Mission & Values<br>• E&C Program Structure<br>• Code of Conduct<br>• Policies and Procedures<br>▪ Internal Investigations<br>▪ Conflicts of Interest<br>▪ Non-Retaliation<br>▪ Social Media<br><br>**External Focused**<br>• Corporate Social Responsibility<br>• Sustainability<br>• Vendor Management<br><br>**Voluntary Standards**<br>• U.S. Federal Sentencing Guidelines<br>• Industry Codes<br>• PCI<br>• Trade Associations<br><br>**Emerging Issues?** |

19

19

# Risk Identification – *Things that Affect Risk*

- Global operations, expansion, and differing cultures
- Financial and other related business demands
- Technology – *Internal/External*
- Economy/Competition/Consumer Demand
- Marketing and other business activities
- Mergers/Joint Ventures/Acquisitions/Alliances
- Laws/Rules/Regulations
- Emerging trends and industry practices
- Leadership/Management changes and turnover
- Unknowns

***Other?***

20

20

# Risk Identification – *Defining Inherent and Control Risks*

| | |
|---|---|
| **Inherent Risk** | **The probability of loss arising out of circumstances or existing in an environment, in the absence of any action to control or modify the circumstances. *Business Dictionary.com*** |
| **Control Risk** | **Probability of loss arising from the tendency of internal control systems to lose their effectiveness over time, and thus expose (or fail to prevent exposure of) the assets they were instituted to protect. *Business Dictionary.com*** |
| **Residual Risk** | **The risk that remains after management's response to the risk. *COSO's Integrated Risk Management – Integrated Framework*** |

***Examples…***

21

21

# Risk Identification – *Internal and External Inputs*

***Sample Internal Inputs***

- Management input, surveys, interviews
- Internal Audit and other functional Risk Management efforts
- Past internal incidents, investigations, audits, risk profiles
- Business operations, operating locations, etc.
- Technology, Security, and other functional areas

***Sample External Inputs***

- Legal/Regulatory requirements
- Enforcement activity and trends
- Social Media and market-place trends
- Industry benchmarking and practices
- Cultural considerations

***Other?***

22

22

## Identified Risks and Next Steps

- **Evaluate Risks** – Consider how risk plays out in the business (*e.g., impact regulatory status, reputation, can it lead to prosecution, etc.*). What are the enforcement trends?
- **Consider Culture and Values** – Tone at the Top, employee trust and morale, influences on culture, how values, ethics, and standards are embedded in the business, etc.
- **Consider Ethical Fault Lines** - Conflicting stakeholder obligations, pressures on business to meet quotas, state of compliance in the industry
  - Are ethical standards compromised in the organization?
  - Do employees feel pressure to make the numbers at any cost?
- **Management Support, Planning and Next Steps**
  - Establish Risk Assessment coverage and initiate activities

23

23

## III. Risk Scenario #1

24

24

## Risk Scenario #1

You have just been hired as the first E&C Risk Officer for a large, global pharmaceutical company. Over the past five years, the organization has acquired 25 smaller firms around the world, but given more pressing business priorities, allows the firms to maintain their existing E&C infrastructures and related risk management programs until resources and budgets are available to fully integrate them into the parent company. To help minimize the financial impact of your new position, the company decides to raise the cost of its popular, life-saving cancer drug by 5000%.

What immediate question would you have, and what potential issues and considerations come to mind? What recommendations will you make?

25

25

## Identified Risks and Universe… *Now what?*

26

26

# IV. Risk Assessment and Prioritization

27

27

## E&C Risk Assessment and Prioritization

***Primary Practice Considerations***

- Value of management input and importance of objectivity
- Solid Risk Assessment methodology in place; ensure coverage of identified risks and scope
- Ensure all Risk Assessment participants are engaged and understand objectives
- Launch, implement and drive a coordinated Risk Assessment effort; provide oversight
- Assess findings and prioritize risk; validate, document and report
- Initiate Risk Management and mitigation planning activities

28

28

# E&C Risk Assessment and Prioritization

### *Legal Privilege and Risk Assessments*

- Legal privilege addresses an assertion to protect certain work product from disclosure when created under direction of counsel for legal purpose
  - Protections *not guaranteed;* impacted by process, waivers (*voluntary and involuntary*), enforcement trends, applicability in global settings
- To maximize likelihood of maintaining privilege:
  - Counsel asserting privilege directs resources to maintain privilege
  - All persons involved in the process are aware of legal purpose and required to maintain confidentiality throughout
  - Work product/reports are general, summarized and include legal opinions where appropriate. Work materials are discarded when purpose served
  - Appropriate labeling of all materials with privilege designation

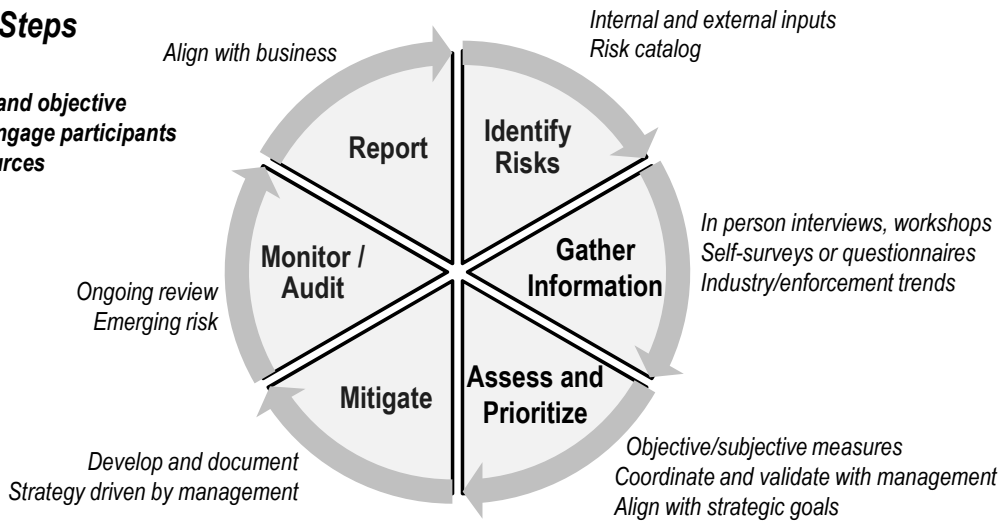
29

29

# Conducting a Risk Assessment

### *Key Process Steps*

- ***Define scope and objective***
- ***Identify and engage participants***
- ***Confirm resources***




30

30

# Conducting a Risk Assessment

***Establish a Risk Assessment Leader***

***Key Attributes:***

- Keen knowledge of the business and operations
- Understanding of general laws, regulations and guidelines driving the business
- Demonstrated leadership, empowerment, and influence in the organization
- Strong decision-making, analytical, and project management skills
- Protects confidential and sensitive information
- Ability to commit and dedicate time to activity

31

31

# Conducting a Risk Assessment

***Establish a Risk Assessment Leader***

***Key Responsibilities:***

- Manage and drive general Risk Assessment activities
- Facilitate engagement with business leaders and unit managers
- Validate key management input for Risk Assessment impact and likelihood
- Provide input on management controls and effectiveness
- Oversee and support Risk Management and Mitigation Action Plans

32

32

# Conducting a Risk Assessment

### *Select Risk Assessment Participants*

***Identification:***

- Leaders/managers in the business with knowledge and influence
- Target audience in business to meet Risk Assessment objectives
- Subject-matter experts, counsel, consultants as needed

***Engagement:***

- Provide input on risk, management controls, and effectiveness
- Help to validate findings and input for Risk Assessment impact/likelihood
- Support Risk Management and Mitigation Action Plans
- Ensure confidentiality and secure sensitive information

33

33

# Assess Findings & Prioritize Risk

### *Risk Impact and Likelihood*

| | |
|---|---|
| **Impact** | **Damage, injury, liability, loss or other negative occurrence that is caused by external or internal vulnerabilities. *(http://www.businessdictionary.com/definition/risk.html*** |
| **Likelihood** | **Likelihood is the chance that something might happen. Likelihood can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively (using mathematics). *ISO 13000 Risk Management Dictionary (http://www.praxiom.com/iso-31000-terms.htm*)** |

34

34

# Assess Findings & Prioritize Risk

## *Risk Impact and Likelihood: Ranking Considerations*

- ***Impact*:** Potential effect that a risk could have on the organization if it arises. Not all threats will have the same impact as each system in the organization may have differing values
  - **High**: Serious impact on operation, reputation, or funding status
  - **Medium**: Significant impact on operations, reputation, or funding status
  - **Low**: Less significant impact on operations, reputation, or funding status

- ***Likelihood*:** Probability that a risk can occur. Factors taken into account in the determination of likelihood are: Source of the threat, capability of the source, nature of vulnerability and existence and effectiveness of current controls. Consider using a scale to help rank such as 1 – 5
  - **High**: An event is expected to occur in most circumstances
  - **Medium**: An event will probably occur in many circumstances
  - **Low**: An event may occur at some time

*A combination of likelihood and impact provides a value for each risk factor and supports prioritization*

***Source***: *World Intellectual Property Organization; http://www.wipo.int/about-wipo/en/oversight/audit/risk_assessment.html*

35

35

# Assess Findings & Prioritize Risk

## Map Risk Assessment Findings and Prioritize*: Define Criteria First and then Rank - High, Medium, and Low*

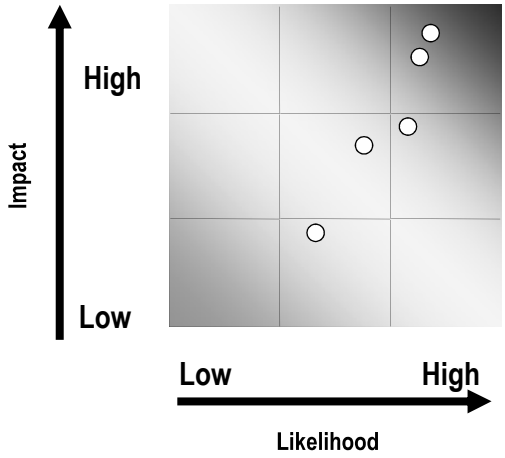
| | Reputation | Legal/Regulatory | Financial |
|---|---|---|---|
| **High** | Systemic loss of public/client confidence resulting in loss of customers; major media coverage – headline news for several days | Major infraction resulting in criminal or civil prosecution and/or significant discipline; loss of ability to operate in one or more countries | Significant financial impact with widespread liability |
| **Medium** | Loss of confidence among large number of customers and a segment of the general public; major media coverage for 1-2 days | Infraction resulting in civil prosecution and/or discipline; loss of ability to operate within local jurisdiction | Considerable financial impact with regional liability |
| **Low** | Loss of confidence among a limited number of customers in local market/country; limited local media coverage | Minor infraction that is readily remediated; no loss of ability to operate | Minimal financial impact with localized liability |

36

36

## Assess Findings & Prioritize Risk – *Sample Heat Map*

***Mapping Inherent Risks – Impact & Likelihood***



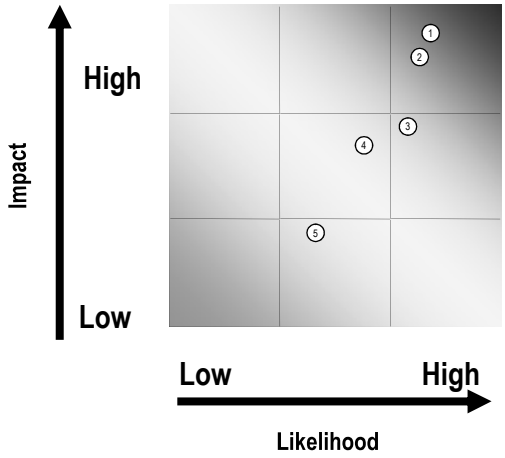

**Circles represent five identified inherent risks mapped by impact and likelihood**

37

37

## Assess Findings & Prioritize Risk – *Sample Heat Map*

***Prioritizing Inherent Risks – Impact & Likelihood***



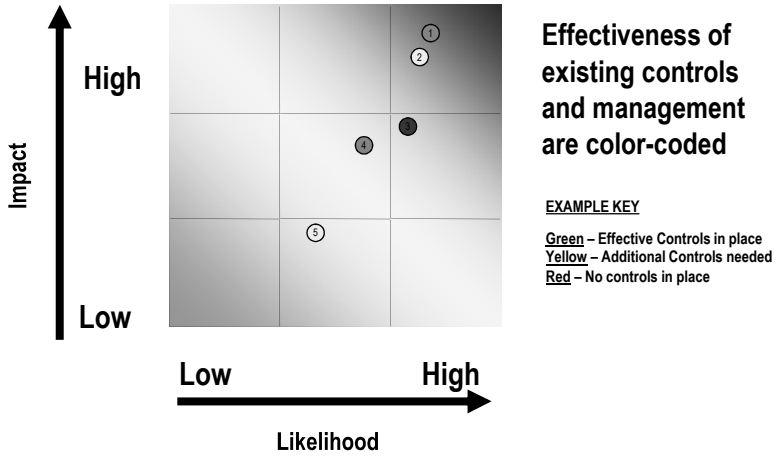

**Inherent risks are prioritized based on impact and likelihood**

38

38

# Assess Findings & Prioritize Risk – *Sample Heat Map*

***Risk Assessment Results – Management Effectiveness/Controls***




**Effectiveness of existing controls and management are color-coded**

**EXAMPLE KEY**

**Green – Effective Controls in place**
**Yellow – Additional Controls needed**
**Red – No controls in place**

39

39

# Assess Findings & Prioritize Risk – *Managing Results*

**Risk Assessment Findings: *Next Steps***

- Coordinate and validate findings and prioritization with management, leadership, specific business units, etc., as applicable
- Organize and consolidate Risk Assessment findings and mapping for broader portfolio view, management efforts, reporting, etc.
- Initiate Risk Management and mitigation planning activities

40

40

# V. Risk Scenario #2

41

41

## Risk Scenario #2

A large, global company that manufactures and distributes office supplies is hiring its first E&C officer to establish a risk management function with a charter to prioritize and manage the organizations' top ethics and compliance risks. During the interview, the General Counsel informs you that the position will be expected to address Health Insurance Portability and Accountability Act (HIPAA) and product Quality Control (QC) risks as top priorities before allocating any time, budget, and resources in other areas.

What immediate questions would you have for the General Counsel?
What recommendations will you make?

42

42

43

43

# VI. Risk Management & Mitigation Strategies

44

44

# Risk Management & Mitigation Strategies

## *Risk Tolerance/Threshold*

| | |
|---|---|
| **Risk Appetite** | **The level of risk that an organization is prepared to accept, before action is deemed necessary to reduce it. It represents a balance between the potential benefits of innovation and the threats that change inevitably brings on. *(http://en.wikipedia.org/wiki/Risk_appetite)*** |

45

45

# Risk Management & Mitigation Strategies

## *Risk Response: Approach Considerations*

- Various frameworks exist that offer approaches to identifying, analyzing, responding to, and monitoring risks and opportunities
- Generally, management will select a *risk response strategy* for prioritized and specific risks identified and analyzed, which may include:

| | |
|---|---|
| **Avoidance** | • Exiting the activities giving rise to the risk |
| **Reduction** | • Taking action to reduce likelihood or impact related to risk |
| **Share or Insure** | • Transferring/sharing a portion of the risk to finance it |
| **Accept** | • No action is taken due to cost/benefit analysis |

***Source:*** ERM Frameworks Defined - http://en.wikipedia.org/wiki/Enterprise_risk_management

46

46

# Risk Management & Mitigation Strategies

***Enabling Effective Action Plans – Primary Considerations***

- **Prioritize** needs based on impact, likelihood, and effectiveness of existing controls in place; determine risk response strategy and develop plans
- **Collaborate** with oversight team/leadership on overall planning and resources for managing/mitigating prioritized risks to include timing, strategic planning, risk response strategy, etc.
- **Assure** accountability and ownership: Risk management owners in business are assigned and specific Risk Management Plans are created and implemented
- **Secure** leadership engagement and support
- **Engage** in ongoing oversight, monitoring and reporting activities

47

47

***Don't dig yourself into a hole…***
*Management is responsible for managing and mitigating risks!*

48

48

## Risk Management & Mitigation Strategies

### *Sample Risk Mitigation Controls*

- Implementing new or improved policies and procedures
- Targeted training and education
- Stronger / automated internal controls
- Organization structure changes
- Performance management / goal setting
- Leveraging Technology

### *Other?*

49

49

## Risk Management & Mitigation Strategies

### *Reporting Activities - Considerations*

- **Audience**
  - Board, Leadership Team, CECO, GC, Compliance Committee, Business Units, Other…
- **Organization Type**
  - Public entity (*e.g., public company reporting requirements, etc.*)
- **Risk Management/Mitigation Plans**
  - Provide periodic and ongoing updates and reporting on status; metrics shared should be focused, measurable, and relevant
  - Include open action plans, owners, target dates, status/progress, etc.

50

50

## Risk Management & Mitigation Strategies

***Reporting Activities – Considerations (Cont.)***

- **Reputation**
  - What is the reputational impact of risk management failures and breakdowns? (*e.g., shareholders, customers, employees*)
- **Business Concerns and Legal Liabilities** (*due diligence activity, litigation, business impact of catastrophic events occurring*)
- **Tone of Reporting** (*keep reporting positive and upbeat where possible*)
- **Report Format/Technology** (*paper or electronic, summary version or detail; follow established and applicable Records Management guidelines/policies*)

51

51

# VII. Monitoring, Auditing, and Follow-up

52

52

# Monitoring, Auditing, and Follow-up

***Process and Management Considerations***

- Oversee, monitor and track Risk Management Plans to completion
- Conduct periodic auditing of Risk Management/Mitigation controls
- Schedule and conduct subsequent and periodic Risk Assessments to ensure ongoing effectiveness
  - Frequency based on evolving business, risk priorities, etc.
- Engage in ongoing monitoring, auditing, and reporting activities

53

53

***Key Take-Aways:***

- ✓ Promote and champion the value of effective Risk Management practice
- ✓ Identify and understand organizational risks and related obligations
- ✓ Conduct periodic and meaningful risk assessments across the organization and prioritize risks based on organizational impact and likelihood
- ✓ Enable effective risk management strategies and mitigation plans
- ✓ Provide ongoing risk management and assessment reporting to stakeholders that is timely, transparent, and objective
- ✓ Monitor, audit, and follow-up

***"Don't let perfect be the enemy of good"***

54

54

# VIII. Wrap-Up and Final Thoughts

55

55

*"If you ever think you're too small to be effective, you've never been in bed with a mosquito."*

**Anita Roddick**

56

56