Compliance Risk Assessment and Management Workshop

Society of Corporate Compliance and Ethics and
Health Care Compliance Association

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

1

1

Workshop Agenda

Today

- Overview of compliance risk assessment and management
- Identification of compliance risks
- Risk appetite and tolerance
- Assessing severity of compliance risks

Tomorrow

- Assessing internal controls over compliance
- Risk response and mitigation
- Completing the compliance risk management cycle
- Final considerations for success

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

2

2

Attendee Poll – Question 1

- Which of the following best describes the industry/sector of your organization:
  - Healthcare
  - Higher education
  - Manufacturing
  - Technology
  - Financial services
  - Nonprofit (other than higher ed)
  - Outside advisor or legal counsel for compliance programs
  - Government agency
  - Other

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

3

Attendee Poll – Question 2

- Which of the following best describes your role:
  - Compliance professional (In-house)
  - Legal counsel (In-house)
  - Risk management (In-house)
  - Internal Audit
  - External advisor/consultant
  - Other

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

4

Attendee Poll – Question 3

- How long have you been in the compliance and/or risk management profession:
  - 0-2 years
  - 3-5 years
  - 6-10 years
  - 10-20 years
  - More than 20 years

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

5

Attendee Poll – Question 4

- Which of the following best describes the maturity of your organization's compliance risk assessment process:
  - We have not yet conducted a compliance risk assessment
  - We have done them, but they are very basic with a lot of room for improvement
  - We perform them on a regular basis, but the process is in need of improvement
  - We have a pretty strong risk assessment process, but are looking for ways to enhance it further

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

6

I. Compliance Risk Management Introduction & Overview

Greg Triguba, JD, CCEP, CCEP-I

Session Agenda

I. <u>Compliance Risk Management</u> – *Introduction & Overview*

- Value Proposition
  - Benefits
  - Risk Management Expectations Globally
- Risk Culture
  - Importance & Impact
- Compliance Risk Management Programs: *Overview*
  - Defining Compliance Risk Management Practice
  - Risk Management Lifecycle
  - Core Practice Objectives & Partnerships
  - Relationship to ERM, Internal Controls, & Three Lines Model

Value Proposition

9

Value Proposition - *Benefits*

Benefits of Effective Compliance Risk Management:

- ✓ Prevents and detects wrongdoing; reduces risks and liabilities from government inquires and enforcement challenges
- ✓ Integrates and assures top compliance and ethics risks are managed and addressed; contributes to overall organizational strategy, decision-making, operational objectives, and business success!
- ✓ Improves and enhances legal/regulatory compliance and risk responses
- ✓ Provides a comprehensive inventory/portfolio view of compliance and ethics risks; *Risk Universe*
- ✓ Promotes shared-vision with leadership on top risks, resource allocation, risk ownership, etc.
- ✓ Assures the organization is working on the right things, at the right time, and with the right resources
- ✓ Supports continuous improvement efforts

More…

10

Value Proposition – *Risk Management Expectations Globally*

Example U.S. Standards

- **U.S. 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) and (5))*
- **Sample U.S. Government Agencies recognizing importance of Risk Management**
  - DOJ, SEC, DOL, DOE, FTC
  - HHS OIG Compliance Program Guidance
  - Federal Energy Regulatory Commission (*Risk Inventory*)

Value Proposition – *Risk Management Expectations Globally*

Example U.S. Standards

- **U.S. Department of Justice (*June 2020*) – "*Evaluation of Corporate Compliance Programs*"**
  - *Is the corporation's compliance program well designed?*
  - *Is the program being applied earnestly and in good faith? (i.e., Adequate resources and empowered)*
  - *Does the corporation's compliance program work in practice?*
- **DOJ Guidance – Key Risk Considerations:**
  - *"The starting point…is to understand the company's business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks."*
  - *"Prosecutors should also consider the effectiveness of the company's risk assessment and the manner in which the company's compliance program has been tailored based on that risk assessment and whether its criteria are periodically updated."*

Value Proposition – *Risk Management Expectations Globally*

Example U.S. Standards

- **DOJ Guidance – Key Risk Considerations (*Cont.*):**

Uniqueness/Risk Universe *- Size, industry, geographic footprint, locations, regulatory landscape, operations, competitiveness of the market, business partners, engagement with foreign officials, use of third parties, gifts, travel and entertainment expenses, charitable/political donations, and other factors*

- ✓ **Risk Management Process**
  - *Methodology, rationale, information/metrics used; and how it informs the C&E program*
- ✓ **Risk-Tailored Resource Allocation**
  - *Is the organization working on the right things, at the right time, with the right resources?*
- ✓ **Updates and Revisions**
  - *Current Risk Assessment, periodic review/updates, broad coverage, continuous improvement*

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

13

Value Proposition – *Risk Management Expectations Globally*

Example U.S. Standards

- **DOJ Guidance – Key Risk Considerations (*Cont.*):**

- ✓ **Lessons Learned**
  - *Process for tracking/incorporating lessons learned into periodic risk assessments*
- ✓ **Third Party Management**
  - *Risk-Based, Integrated Process, Internal Controls, Relationship Management, Red Flags*
- ✓ **Mergers and Acquisitions (*M&A*)**
  - *Due Diligence Process; Integration Activities; Connecting Due Diligence to Implementation*
- ✓ **Data Resources and Access**
  - *Sufficient access to sources of data and information; address impediments that limit access*
- ✓ **Culture and Management Commitment**
  - *Risk Culture, tone at top/middle, shared commitment, oversight*

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

14

Value Proposition – *Risk Management Expectations Globally*

Example U.S. Standards

- **HCCA-OIG Compliance Effectiveness Roundtable – *"Measuring Compliance Program Effectiveness: A Resource Guide"* (Mar 2017)**

  For Healthcare Organizations:

  - Leverages the USSG Effectiveness Elements and expectations regarding Risk Assessments and Management as a foundation.
  - Similar expectations regarding risk management effectiveness that is addressed in the recent DOJ Guidance and other related resources
    - ✓ Effective framework/infrastructure; documented; integrated into the business; enterprise-wide; risk-based resource allocation; input to monitoring/auditing efforts; partnering with other risk functions (e.g., IA and ERM); leverage findings for continuous improvement, etc.
  - Additionally, OIG-HHS emphasizes and incorporates risk management expectations in its compliance guidance across specific healthcare disciplines (https://oig.hhs.gov).

15

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

15

Value Proposition – *Risk Management Expectations Globally*

Other Global Standards, Guidelines, & Frameworks

- COSO Enterprise Risk Management – Integrated Framework
- NIST Risk Management Framework
- International Organization for Standardization (ISO) (*e.g., 31000, 37001, 37301*)
- Federation of European Risk Management Associations (FERMA)
- French Anticorruption Agency (AFA) – *French Sapin II Law*
- Singapore Investigations Bureau – *The Prevention of Corruption Act*
- Brazil Clean Companies Act
- UK Bribery Act and U.S. Foreign Corrupt Practices Act
- OECD Good Practice Guidance
- Competition Bureau Canada – *Corporate Compliance Programs*
- 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

More...

16

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

16

Value Proposition – *Risk Management Expectations Globally*

Example Global Standards

UK Bribery Act 2010 – *Adequate Procedures; Principle 3, "Risk Assessment"*

"The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented."

"Procedures

3.3 *Risk assessment procedures that enable the commercial organisation accurately to identify and prioritise the risks it faces will, whatever its size, activities, customers or markets, usually reflect a few basic characteristics. These are:*

- *Oversight of the risk assessment by top level management.*
- *Appropriate resourcing – this should reflect the scale of organization's business and the need to identify and prioritize all relevant risks.*
- *Identification of the internal and external information sources that will enable risk to be assessed and reviewed.*
- *Due diligence enquiries.*
- *Accurate and appropriate documentation of the risk assessment and its conclusions."*

17

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

17

Value Proposition – *Risk Management Expectations Globally*

Example Global Standards

Organisation for Economic Co-operation and Development (OECD)

- ***Good Practice Guidance on Internal Controls, Ethics, and Compliance (2021)***

  "Effective internal controls, ethics, and compliance programmes or measures for preventing and detecting foreign bribery should be developed on the basis of a risk assessment addressing the individual circumstances of a company, in particular the foreign bribery risks facing the company (such as its geographical and industrial sector of operation, and regulatory environment, potential clients and business partners, transactions with foreign governments, and use of third parties)."

  "…Such circumstances and risks should be regularly monitored, re-assessed, and taken in account as necessary, to determine the allocation of compliance resources and ensure the continued effectiveness of the company's internal controls, ethics, and compliance programme or measures."

- ***OECD, Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions (2021)***

  "Member countries should encourage:

  i. companies, including state-owned enterprises, to develop and adopt adequate internal controls, ethics and compliance programmes or measures for the purpose of preventing and detecting foreign bribery, taking into account the Good Practice Guidance…"

18

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

18

Value Proposition – *Risk Management Expectations Globally*

Example Global Standards

International Organization for Standardization (ISO)

- ***ISO 31000:2018 – Risk Management - Guidelines***

  Provides principles, a framework, and a process for managing risk; can be used by any organization regardless of its size, activity, or sector; helps organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

- ***ISO 37001:2016 – Anti-bribery management systems***

  Standard designed to prevent, detect and address bribery by adopting an anti-bribery policy, appointing a person to oversee compliance, training, risk assessments and due diligence on projects and business associates, implementing financial and commercial controls, and instituting reporting and investigation procedures.

- ***ISO 37301:2021 – Compliance management systems – Requirements with guidance for use***

  Provides guidelines for developing, implementing, evaluating, maintaining and improving an effective compliance management system within an organization; applicable to all types of organizations regardless of type, size and nature of the activity, or whether the organization is from a public, private, or non-profit sector.

Source: *http://www.iso.org*

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Value Proposition – *Risk Management Expectations Globally*

Example Global Standards

COSO - Committee of Sponsoring Organizations of the Treadway Commission

- *Comprised of five private-sector, professional organizations dedicated to helping organizations improve performance through thought leadership and development of frameworks and guidance on internal control, enterprise risk management, governance and fraud deterrence*
- *Originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting; studied causal factors that can lead to fraud and developed recommendations for public companies, SEC, etc.*
- *Known for establishing globally recognized frameworks and guidance on Internal Control and Enterprise Risk Management (ERM); widely used by risk, audit, compliance, and other professionals to more effectively manage and mitigate risk across organizations and prevent fraud*
- *In a joint 2020 collaboration, SCCE/HCCA and COSO introduced a global resource and framework that helps organizations effectively apply the COSO ERM Framework to compliance risk management practice (see, Compliance Risk Management: Applying the COSO ERM Framework)*

Source: *http://www.coso.org*

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Value Proposition – *Risk Management Expectations Globally*

https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

21

Risk Culture

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

22

Risk Culture – *Importance & Impact*

Defined:

"Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose. This applies to all organisations - including private companies, public bodies, governments and not-for-profits." Institute of Risk Management (www.theirm.org)

"Risk Culture denotes the combined set of Corporate Values, norms, attitudes, competencies and behavior related to risk awareness (perception of risk) and risk taking (active business decisions) that determine a firm's commitment to and style of Risk Management." Open Risk Manual (www.openriskmanual.org)

Notable Scandals:

- *Wells Fargo*
- *Citigroup*
- *Tenet Health*
- *Sutter Health*

Risk Culture – *Importance & Impact*

Importance of a strong Risk Culture:

- ✓ Board engagement and oversight;
- ✓ Leadership tone and commitment; Tone in the Middle; Buzz at the Bottom
- ✓ Aligned core values; *accountability at all levels*
- ✓ Positive perceptions of leadership, organizational justice, core values, integrity, and ethics
- ✓ Periodic culture assessments, surveys, and related touch-points
- ✓ Speak-up culture; employees feel safe seeking help and reporting concerns
- ✓ Meaningful risk management infrastructure and framework; *integrated into DNA*
- ✓ Strong risk awareness across the organization; ongoing training and communication
- ✓ Continuous improvement/enhancement to compliance risk management infrastructure

Compliance Risk Management Programs

25

Defining Compliance Risk Management Practice

Risk	**"The possibility that events will occur and affect the achievement of strategy and business objectives. Risks considered in this definition include those relating to all business objectives, including compliance."** **Compliance Risk Management: Applying the COSO ERM Framework ©2020, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.**
Compliance Risk	**"Compliance risks are those risks relating to possible violations of applicable laws, regulations, contractual terms, standards, or internal policies where such violations could result in direct or indirect financial liability, civil or criminal penalties, regulatory sanctions, or other negative effects for the organization or its personnel."** **Compliance Risk Management: Applying the COSO ERM Framework ©2020, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.**

26

Defining Compliance Risk Management Practice

Enterprise Risk Management	"Enterprise risk management (ERM) is a methodology that looks at risk management strategically from the perspective of the entire firm or organization. It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentials for harm that may interfere with an organization's operations and objectives and/or lead to losses." Investopedia (www.investopedia.com/terms/e/enterprise-risk-management.asp) "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." Enterprise Risk Management – Integrating with Strategy and Performance ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.
Risk Management	"Risk management encompasses the identification, analysis, and response to risk factors that form part of the life of a business. Effective risk management means attempting to control, as much as possible, future outcomes by acting proactively rather than reactively. Therefore, effective risk management offers the potential to reduce both the possibility of a risk occurring and its potential impact." Corporate Finance Institute (http://corporatefinanceinstitute.com)

Defining Compliance Risk Management Practice

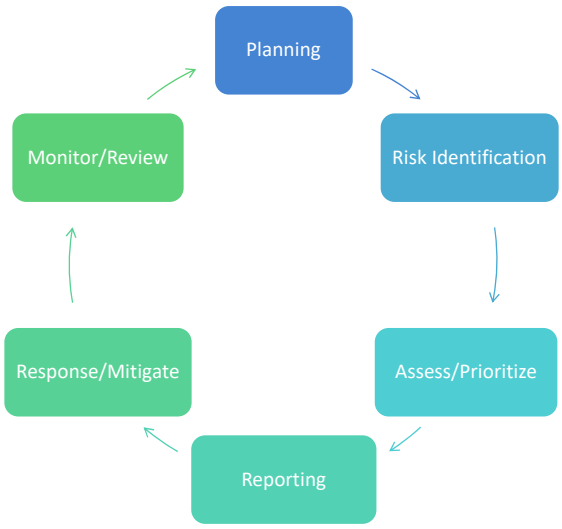
Risk Assessment	A risk assessment includes the processes of identifying, analyzing, and evaluating the likelihood and severity of risks. Performing these steps helps determine the best way to address those risks: to monitor, minimize, or mitigate their impact. Compliance Risk Assessments – An Introduction Society of Corporate Compliance & Ethics (©2020) (https://compliancecosmos.org/chapter-2-risk-assessment-and-risk-management-primer)
Internal Control	"Internal control is 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." COSO Internal Control – Integrated Framework ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used with permission.

Defining Compliance Risk Management Practice

Risk Appetite/Tolerance - Introduction

Risk Appetite	**"The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value."**
Risk Tolerance	**"The boundaries or acceptable variation in performance related to achieving business objectives."**

Risk Management Lifecycle – *Overview*



Key Steps

- ✓ Planning/Scope
- ✓ Risk Identification
- ✓ Assess/Prioritize
- ✓ Reporting
- ✓ Risk Response/Mitigate
- ✓ Monitor/Review

❖ *Continuous Improvement*

Risk Management Lifecycle – *Practice Objectives*

Lifecycle - Core Practice Objectives:

- Leadership Commitment; Organizational Support; *Strong Risk Culture*
- Solid infrastructure, planning and implementation strategies in place
- Parties involved are engaged and understand objectives
- Meaningful risk identification and scoping activities; understanding of Risk Universe
- Effective methodology, 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; *Continuous Improvement*

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Risk Management Lifecycle – *Partnerships*

Lifecycle – Key Partnerships and Teams

- Governing Body/Senior Leadership
- CECO, General Counsel, Legal/Compliance SMEs
- Functional Group Partners: IT, HR, Finance, Internal Audit, Info Security, , etc.
- Business/Operating Unit Representation: Leadership, management teams, regional managers, global locales, etc.
- Designated Risk Assessment Leaders and teams
- Consultants and other external SMEs as needed

Other Partners…

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

Compliance Risk Management – *Relationship to ERM & Internal Controls*

Relationship to ERM Framework…

- COSO defines ERM: "*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.*" Compliance Risk Management: Applying the COSO ERM Framework (©2020) (www.coso.org)

✓ **Effective Compliance & Ethics Programs and related risk management help organizations to mitigate and minimize risk and liabilities associated with compliance failures, and these efforts directly, and indirectly, help enable organizations to focus more on opportunities that create, preserve, and realize value.**

Five components supported by 20 principles

Source: COSO Enterprise Risk Management – Integrating with Strategy and Performance 2017

33

Compliance Risk Management – *Relationship to ERM & Internal Controls*

Relationship to ERM Framework…

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 2017

34

Compliance Risk Management – *Relationship to ERM & Internal Controls*

Relationship to Internal Control Framework…

- *"Internal control is 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."* COSO Internal Control – Integrated Framework (©2013) (www.coso.org)

✓ **Compliance with laws, regulations, and mitigation of compliance-related risks is a fundamental objective of an organization's internal control system, and is supported throughout the organization by five key components of internal control support, efforts, and activities.**

Three Objectives

Five Components

At Various Org. Levels

Source: COSO Internal Control Framework 2013

SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

35

35

Compliance Risk Management – *Relationship to IIA's Three Lines Model*

IIA's Three Lines Model (2020) - *Overview*

- Assists organizations in identifying structures and processes that enable the achievement of objectives and facilitate strong governance and risk management
- Enables organizations to better structure interactions and responsibilities of management, internal audit, and the governing body to more effectively and efficiently create and protect value
  - Roles are better aligned with each other on risk management priorities and stakeholder interests
  - Alignment is achieved through collaboration, communication, cooperation to ensure reliability and transparency that improves risk-based decision making
- Model supports a direct reporting line to the governing body by the CCO or CRO (*similar to Internal Audit*)
- Identifies responsibilities at:
  - **Governing body** – *Oversight Responsibilities*
  - **Management, including Operational Leaders like Risk and Compliance** – *First- and Second-Line Roles*
  - **Internal Audit** – *Third-Line Role (Independent Assurance)*
  - **External Assurance** – *Additional Assurance*
- First-Line management roles are responsible for managing risk, whereas Second-Line management roles serve to provide complementary expertise, support, monitoring, etc., to First-Line roles (e.g., C&E, ERM, HR)

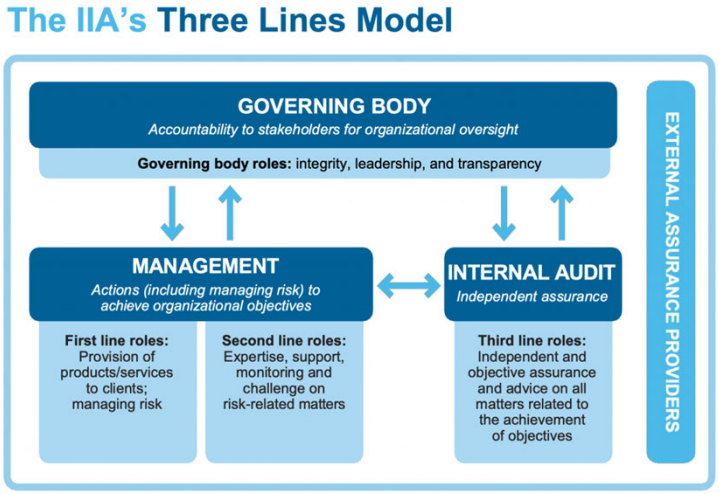
SCCE Society of Corporate Compliance and Ethics

HCCA Health Care Compliance Association

36

36

Compliance Risk Management – *Relationship to IIA's Three Lines Model*



Source: ***The IIA's Three Line Model***

37

37

Compliance Risk Management – *ERM, IC, and Three Lines Model*

Elements of an Effective Compliance & Ethics Program

- ✓ Culture and Values
- ✓ Standards and Procedures
- ✓ Governance, Oversight, and Authority
- ✓ Due Care in Delegation of Authority
- ✓ Training and Communication
- ✓ Monitoring, Auditing, and Reporting Systems
- ✓ Incentives and Enforcement
- ✓ Response to Wrongdoing and Remedial Measures
- ✓ Periodic Risk Assessment
- ✓ Continuous Program Improvement

38

38

Compliance Risk Management – *ERM, IC, and Three Lines Model*

Relationship to ERM, Internal Controls, and Three Lines Model

- Effective Compliance & Ethics Program Elements share numerous characteristics that are central to key objectives of ERM, Internal Controls, and Three Lines Model.

Examples include:

- ✓ Importance of effective risk management infrastructures and processes
- ✓ Strong governance structures in place; commitment and engagement
- ✓ Standards, policies, and procedures in place to support risk management
- ✓ Value of culture to effectiveness; *Risk Culture*
- ✓ Importance of ongoing communications and reporting
- ✓ Effective response to risk and remedial measures
- ✓ An expectation of continuous program improvement

Compliance Risk Management – *Introduction/Overview*

NEXT SESSION – *IDENTIFICATION OF COMPLIANCE RISK*

15 MINUTE BREAK