Ethics & Compliance Risk Management 101: 
Program Essentials and Effective Practice 
*Key Steps to Implementing and Championing an Effective Program*

Greg Triguba, JD, CCEP 
Sheryl Vacca, CCEP, CCEP-I, CHC-F, CHRC, CHPC

---

**Workshop Agenda**

I. Ethics & Compliance Risk Management Overview
   - Value Proposition
   - Risk Management Essentials: *Getting Started*
     - Defining Risk Management Practice
     - Primary Practice Considerations
     - 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 Assessment and Prioritization

- Primary Practice Considerations
- Legal Privilege and Risk Assessments
- Conducting a Risk Assessment
  - Key Process Steps and Considerations
  - Establishing a Risk Assessment Leader
  - Selecting Risk Assessment Participants
- Assess Findings and Prioritize Risk
  - Risk Impact and Likelihood: Organizational Tolerance/Thresholds
  - Map Risk Assessment Findings and Prioritize
  - Management Review and Input

IV. Group Exercise: Identifying and Prioritizing Risk

V. Risk Management and Mitigation Strategies

- Effective Risk Management Practice
  - Risk Response: Approach Considerations
  - Enabling Effective Action Plans
  - Sample Risk Management Controls
  - Reporting Activities

VI. Monitoring, Auditing, and Follow-up

- Primary 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

VII. Wrap-Up and Final Thoughts
I. Ethics & Compliance Risk Management Overview
Ethics & Compliance Risk Management Overview - Value Proposition

Benefits of Effective Risk Management Practice:

- Portfolio view of compliance and ethics risks; allows for effective identification, prioritization and management
- 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 and 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

Risk Management enables Compliance

- 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."
  - Risk management elements: Standards and Procedures (Internal Controls), monitoring, auditing, periodic evaluation (§8B2.1(b)(1)(5))
- Sample Federal Agencies recognizing importance of Risk Management
  - DOL, DOE, FTC
  - HHS OIG Compliance Program Guidance
  - Federal Energy Regulatory Commission (Risk Inventory)
  - NIH, NSF, etc.
“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

Ethics & Compliance 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](https://www.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](https://en.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](https://www.businessdictionary.com)

**Other Definitions?**
I feel like I'm drowning

Ethics & Compliance Risk Management Overview – Practice Essentials

Primary Risk Management Practice Considerations

- Leadership and Organizational Support
- 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 documenting findings and prioritizing risks
- Enable and oversee effective risk mitigation and management plans; drive ownership and accountability throughout the business
- Monitor, Audit, Report, and Follow-up
Ethics & Compliance Risk Management Overview - Practice Essentials

Key Risk Management 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, etc.
- Designated Risk Assessment Leader and staff
- Consultants and other external SME’s as needed

Other Partners?
II. Risk Identification

Risk Identification - Organizational Risks and Universe

*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
Risk Identification - *Organizational Risks and Universe*

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

**Things that Affect Risk**
- Global Operations and Differing Cultures
- Financial and Other Business Demands
- Technology
- Competition
- Marketing
- Mergers/Joint Ventures/Acquisitions/ Alliances
- Laws/Rules/Regulations
- Unknowns

*Other?*
Risk Identification - Organizational Risks and Universe

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. [BusinessDictionary.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. [BusinessDictionary.com]

Risk Identification - Organizational Risks and Universe

Internal and External Inputs

**Sample Internal Inputs**

- Management Input
- Internal Audit and other functional Risk Management efforts
- Past Internal Incidents, Investigations, and Risk Profiles
- Business Operations, Operating locations, etc.
- Technology, Security, and other functional areas

**Sample External Inputs**

- Legal and Regulatory Requirements, and Enforcement Activity
- Market-place trends and Social Media
- Industry benchmarking and practices

**Other?**
Risk Identification - Organizational Risks and Universe

Risk List – Where do we go from here?

- Analyze Risks - How do risks play out in the business (e.g., which affect regulatory status, reputation, can lead to prosecution, what are enforcement trends?)
- Consider Cultural Influences – Tone at the Top, employee trust, business metrics, compensation plans, external influence on culture
- Consider Ethical Fault Lines - Conflicting stakeholder obligations, state of compliance in the industry
  - Is non-compliance accepted?
  - Do employees believe that they can both comply and compete?
- Management Support, Planning and Next Steps
  - Establish Risk Assessment coverage and initiate activities
III. Risk Assessment and Prioritization

Ethic & Compliance Risk Assessment and Prioritization

Primary Practice Considerations

- Value of management input and importance of objectivity
- Use of Legal Privilege in the Risk Assessment process
- 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
Ethics & Compliance Risk Assessment and Prioritization

Legal Privilege and Risk Assessments

- Legal privilege generally addresses an assertion to legally protect certain internal work product from disclosure when created under the direction of counsel for a legal purpose
  - Three Types: Attorney-Client, Work-Product, and Self-Critical Analysis
  - Protections not guaranteed and impacted by process, waivers (voluntary and involuntary), government enforcement trends, applicability in global settings
- To maximize likelihood of maintaining privilege:
  - All persons involved in the process are aware of the legal purpose at the beginning of the RA and required to maintain confidentiality throughout
  - Counsel asserting privilege retains and directs resources to maintain privilege
  - Work product and reports are general, summarized and include legal opinions and impressions where appropriate. Work materials leading to summary are discarded when purpose served
  - Appropriate labeling of all materials with privilege designation

Risk Assessment and Prioritization - Conducting the Risk Assessment

Key Process Steps and Considerations

- Leverage risk identification output and ensure coverage
- Identify and engage Risk Assessment participants and resources
- Initiate Risk Assessment activity to include gathering input on risks, organizational impact, likelihood, and effectiveness of any management controls
- Utilize established risk-focused questionnaires and related tools
- Collaborate with leaders on overall findings, reporting and next steps
- Identify areas of impact and initiate risk management/mitigation planning
Risk Assessment – Establishing a Risk Assessment Leader

*Individual appointed to Oversee and Drive Risk Assessment*

**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 and analytical skill-set
- Protects confidential and sensitive information
- Ability to commit and dedicate time to activity

---

Risk Assessment – Establishing 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
- Support Risk Management and Mitigation Action Plans
Risk Assessment – Selecting 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 Mitigations Action Plans
• Ensure confidentiality and secure sensitive information

Risk Assessment and Prioritization – Assess Findings & Prioritize Risk

Risk Impact and Likelihood – Organizational Tolerance/Thresholds

- 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](http://en.wikipedia.org/wiki/Risk_appetite)

- Risk Impact: Damage, injury, liability, loss or other negative occurrence that is caused by external or internal vulnerabilities. [http://www.businessdictionary.com/definition/risk.html](http://www.businessdictionary.com/definition/risk.html)

- Risk 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](http://www.praxiom.com/iso-31000-terms.htm)
Risk Assessment and Prioritization – Assess Findings & Prioritize Risk

Risk Likelihood and Impact: Ranking Considerations

- **Risk 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. Likelihood can be described as high, medium and low.
  - **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

- **Risk 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 is worth differently. The magnitude of impact also can be categorized as high, medium and low.
  - **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

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


---

Risk Assessment and Prioritization – Assess Findings & Prioritize Risk

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

<table>
<thead>
<tr>
<th>Reputation</th>
<th>Legal/Regulatory</th>
<th>Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Systemic loss of public interest confidence resulting in loss of customers, major media coverage - headline news for several days</td>
<td>Major infraction resulting in criminal or civil prosecution and/or significant discipline, loss of ability to operate in one or more countries</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Loss of confidence among large number of customers and a segment of the general public, major media coverage for 1-2 days</td>
<td>Infraction resulting in civil prosecution and/or discipline, loss of ability to operate within local jurisdiction</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Loss of confidence among a limited number of customers in local market/country, limited local media coverage</td>
<td>Minor infraction that is readily remediated, no loss of ability to operate</td>
</tr>
</tbody>
</table>
Risk Assessment and Prioritization – *Sample Heat Map*

**Mapping Inherent Risks – Impact & Likelihood**

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

Risk Assessment and Prioritization – *Sample Heat Map*

**Prioritizing Inherent Risks – Impact & Likelihood**

Inherent risks are prioritized based on impact and likelihood.
**Risk Assessment and Prioritization – Sample Heat Map**

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

Effectiveness of existing controls and management are color-coded

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

---

**Risk Assessment and Prioritization – 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
IV. Group Exercise: *Identifying and Prioritizing Risk*

V. Risk Management & Mitigation Strategies
Risk Management and 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 a cost/benefit decision


Risk Management and 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.

- Risk Management Leader collaborates with oversight team/leadership on overall planning and resources for managing/mitigating prioritized risks to include timing, strategic planning, risk response strategy, etc.

- Risk Management owners in business are assigned and specific Risk Management Plans are created and implemented; ensure accountability and ownership.

- Ensure leadership engagement and support.

- Engage in ongoing oversight, monitoring and reporting activities.
Don't walk the tightrope between Management and Compliance - Management is responsible for managing and mitigating risks!

Risk Management and Mitigation Strategies

Sample Risk Management Controls

- Holding management accountable for remediating risk
- Monitoring by compliance and/or management tools
- Training and education
- Implementing policies and procedures
- Compliance validates and/or audits process
- Technology

Other?
Risk Management and Mitigation Strategies

Reporting Activities - Considerations

- Audience?
  - Board, Management, Business Units, Other

- Organization Type
  - Public entity (e.g., intranet vs. public website, etc.)

- Reputation
  - What would someone say if they saw your results? (e.g., shareholders, customers, staff)

- Business Concerns and Legal Liabilities (e.g., due diligence activity, litigation, catastrophic event occurring)

- Report Format and Technology (e.g., paper or electronic, summary version or detail)

VI. Monitoring, Auditing, and Follow-up
Monitoring, Auditing, and Follow-up

*Primary 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

VII. Wrap-Up and Final Thoughts
“If you ever think you're too small to be effective, you've never been in bed with a mosquito.”

Anita Roddick

In Conclusion…

“The greater danger for most of us lies not in setting our aim too high and falling short; but in setting our aim too low, and achieving our mark.”

Michelangelo