RISK ASSESSMENT: More, Wider, Deeper

Sally March and Ruth Steinholtz
SCCE European Compliance and Ethics Institute
March 2015

Agenda

› Basic Compliance Risk Assessment

› Ethics and Culture Risk
  ◦ What are they?
  ◦ Why is this important?

› Assessing Ethics and Culture Risk
CCO’s Responsibilities

- #1 Ensure the Business understands its risks and manages them appropriately
  - Ensure periodic C&E risk assessments are conducted across the organization
  - Drive the integration of C&E risk assessments across the Business Units
  - Ensure that risks are appropriately prioritized
  - Ensure that action plans are developed and carried out on risk assessments
  - Evaluate risk mitigation

COSO ERM Framework

- Event Identification
  - Risk Assessment - evaluate likelihood and impact
  - Risk Response - avoid, accept, reduce, share
  - Control Activities - based on risk evaluation, identify and implement mitigation activity

Monitoring - revisit established controls on a periodic basis to ensure they are effective and working as designed and that they continue to be relevant.

Audit Universe

Assess and Respond
Conducting Effective Risk Assessments

› **Preparation**
  - Get executive buy-in. This is strategic and goes to the heart of the organisation’s ability to realise its objectives.
  - Understand your organisation and its activities, e.g., lines of business, key business risks, recent business changes, likely business changes, strategies, competitors, industry practices, geography/dispersion.
  - Where are key decisions made that can create risk?
  - Understand your organisation’s ERM framework.
  - Planning and Methodology – the process methodology must be objective and defensible.
  - Who will conduct the assessment? Field a diverse team. Do you need external consultants?
  - Consider the need for legal privilege, protocols for document creation.

› **Scope**
  - Examine all major areas of E&C risk, “gross”
  - Don’t forget the “E”
    - Ethics, Culture and Code of Conduct
    - Criminal conduct
    - Legal and regulatory
    - Policies and procedures
    - Industry standards
    - Are you capturing activities that are questionable though not illegal?
  - Address both current and potential risks –

  “Predicting the past with 90% accuracy”
Conducting Effective Risk Assessments

› Interviews & Document Review

- Risk assessments should involve participants from all parts of the business and from all levels.
- Assess the ability of leaders to recognize and prevent compliance failures.
- How are you going to assess “tone” and culture?
- Internal corporate documents
- External industry reports and other sources, e.g., TI CPI
- Include “near misses” as well as failures

› Qualify, Quantify and Validate

- Likelihood that risk will occur
- Impact if it does
  - Type of impact, e.g., prosecution, civil damages, reputational damage, management time
  - Extent of impact
- Velocity? Other factors?

- Challenge and validation – ultimately the Board or Audit Committee
Conducting Effective Risk Assessments

- Identify control activities
  - For each risk, what are the current controls?
  - Awareness of current controls

- Define further mitigation plans
  - Mitigation plans should reflect risk appetite – avoid, accept, reduce or share
  - High risk and weakest controls -- improve
  - High risk and strong controls -- monitor

- Validate gross vs residual risk
  - Beware false sense security re: residual risk

Assessing Culture Risk

- *Not everything that counts can be counted, and not everything that can be counted counts.* William Bruce Cameron (not Einstein)

- What is culture?

- But, how can we measure something so ____?

- Don’t we need to understand what drives unethical behaviour?
Top Factors most likely to cause unethical behaviour

<table>
<thead>
<tr>
<th>Factor</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressure to meet unrealistic objectives/deadlines</td>
<td>69.7%</td>
</tr>
<tr>
<td>Desire to further one's career</td>
<td>38.5%</td>
</tr>
<tr>
<td>Desire to protect one's livelihood</td>
<td>33.8%</td>
</tr>
<tr>
<td>Environment of cynicism or diminished morale</td>
<td>31.1%</td>
</tr>
<tr>
<td>Improper training/didn't know it was unethical</td>
<td>27.7%</td>
</tr>
<tr>
<td>Lack of consequences if caught</td>
<td>24.3%</td>
</tr>
<tr>
<td>Following boss’s orders</td>
<td>23.5%</td>
</tr>
<tr>
<td>Peer pressure/desire to be a team player</td>
<td>14.9%</td>
</tr>
<tr>
<td>Wanting to help the organisation survive</td>
<td>8.7%</td>
</tr>
<tr>
<td>A sense of loyalty</td>
<td>6.9%</td>
</tr>
<tr>
<td>Desire to steal from or harm the organisation</td>
<td>9.5%</td>
</tr>
</tbody>
</table>

Source: US Management Association 2006; Survey of 1,121 global managers

Values are the building blocks of culture, influencing behaviour

It is possible to measure (and change) culture, using tools that have been around for many years!


**Stages in the Development of Organisational Focus**

![Diagram showing stages of organisational focus]

**Positive Focus**
- Service To Humanity And The Planet
  - Social responsibility, future generations, long-term perspective, ethics, compassion, humility
- Strategic Alliances and Partnerships
  - Environmental awareness, community involvement, employee fulfilment, coaching/mentoring
- Building Corporate Community
  - Shared values, vision, commitment, integrity, trust, passion, creativity, openness, transparency
- Continuous Renewal and Learning
  - Accountability, adaptability, empowerment, teamwork, goals orientation, personal growth
- High Performance
  - Systems, processes, quality, best practices, pride in performance. Bureaucracy, complacency
- Belonging
  - Loyalty, open communication, customer satisfaction, friendship. Manipulation, blame
- Financial Stability
  - Shareholder value, organisational growth, employee health, safety. Control, corruption, greed

**Excessive Focus**

**Full Spectrum Story: Focus on:**

- **Level 7** – Ethical behaviour; doing things because it is the right thing to do. Long term perspective and serving the greater good.
- **Level 6** – Collaborative working environment, win-win outcomes. Focus on leadership development that makes a difference. Sustainability and environmental awareness.
- **Level 5** – Clear vision and the values are lived and demonstrated by the senior team in their decision making. High levels of trust and honesty.
- **Level 4** – Staff feeling engaged and empowered. Business is continually improving and developing.
- **Level 3** – High performing systems. E.g. Fast decisions and accurate order fulfilment. People feel a sense of pride when they tell others who they work for.
- **Level 2** – Satisfied customers and staff. Respectful and open communication.
- **Level 1** – Profitable, financially stable, fair prices and pay? Good working conditions.
The values that are important to employees in their personal lives.

How employees experience the company – What is working well? What is undermining the sustainability of the company.

Leisure and Tourism Example 1 (98)

Level | Personal Values (PV) | Current Culture Values (CC) | Desired Culture Values (DC)
--- | --- | --- | ---
7 | | | |
6 | | | |
5 | | | |
4 | | | |
3 | | | |
2 | | | |
1 | | | |

Matches
PV - CC 1 CC - DC 4 PV - DC 2

Health Index (PL)
PV: 10-0 CC: 7-3 DC: 10-0

IRS (P)= 8-2-0 | IRS (L)= 0-1-0 IROS (P)= 1-4-5-0 | IROS (L)= 0-0-1-0 IROS (P)= 1-5-4-0 | IROS (L)= 0-0-0-0
But my CEO won’t agree to a values survey...

- Keep working on them
- In the meantime, do you have a leadership development or talent management dept?
- Face to face interviews, probing issues such as whether the culture encourages challenge, the quality of leadership, the “atmosphere” in various areas of the company
- Exit interviews, employee surveys, other employee communications

---

1st | Business operations
A robust environment under which processes and controls are effectively operated

- Design, implement and operate systems, process and controls to effectively support decision-making, manage risks, and achieve strategic objectives

2nd | Divisional and group oversight
Consistent monitoring and management of the effective operation of processes and controls

- Establish policies and procedures, roles and responsibilities, boundaries for the operations and tone at the top.
- Oversight functions that monitor, test and resolve control or transactional failures e.g. management operational committees, Compliance and Quality functions, etc.

3rd | Internal Assurance
Independent control environment assessment

- Independent assessment of the effectiveness of business operations and management oversight including second line oversight functions
- Examples include Internal Audit, Security, and Health and Safety Assurance functions
Thank you for listening

Sally J. March, J.D., LL.M., CCEP
Drummond March & Co.
sjmarch10@gmail.com
+44(0)7909915456

Ruth Steinholtz  (see bio for details)
Aretéwork LLP
ruth@aretework.com
+44 (0)7900 681457

Further Reading

- UK Ministry of Justice Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing
- COSO Integrated Risk Management Framework
- “Conducting Effective Risk Assessments”, Association of Corporate Counsel InfoPAK
- Scott Killingsworth, “Some realism about risk assessments”, Compliance & Ethics Professional, January 2015
- Richard Barrett, The Values Driven Organization, Routledge, 2014
- M. Bazerman and A. Tenbrunsel, Blind Spots: Why we Fail to do What’s Right and What to Do about it, Princeton University Press, 2011
- M. Heffernan, Wilful Blindness, Why we ignore the obvious at our peril, Simon & Schuster, 2011
Federal Sentencing Guidelines require risk assessment

- 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.”

Adequate Procedures require risk assessment

- **#1 Proportional Procedures**
  - “Adequate bribery prevention procedures ought to be proportionate to the bribery risks that the organisation faces. An initial assessment of risk across the organisation is therefore a necessary first step.”

- **#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.”

  *Source: UK Ministry of Justice Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing*
OECD Good Practice Guidance on Internal Controls, Ethics, and Compliance

6. Ethics and compliance programmes or measures designed to prevent and detect foreign bribery applicable, where appropriate and subject to contractual arrangements, to third parties...(hereinafter “business partners”), including, inter alia, the following essential elements:
   ◦ i) properly documented risk-based due diligence pertaining to the hiring, as well as the appropriate and regular oversight of business partners;

Sarbanes–Oxley requires risk assessment

- The Public Company Accounting Oversight Board (PCAOB) approved Auditing Standard No. 5 for public accounting firms on July 25, 2007. This standard superseded Auditing Standard No. 2, the initial guidance provided in 2004. The SEC also released its interpretive guidance on June 27, 2007. It is generally consistent with the PCAOB’s guidance, but intended to provide guidance for management. Both management and the external auditor are responsible for performing their assessment in the context of a top-down risk assessment, which requires management to base both the scope of its assessment and evidence gathered on risk. This gives management wider discretion in its assessment approach. These two standards together require management to:
  ◦ Assess both the design and operating effectiveness of selected internal controls related to significant accounts and relevant assertions, in the context of material misstatement risks;
  ◦ Understand the flow of transactions, including IT aspects, in sufficient detail to identify points at which a misstatement could arise;
  ◦ Evaluate company-level (entity-level) controls, which correspond to the components of the COSO framework;
  ◦ Perform a fraud risk assessment;
  ◦ Evaluate controls designed to prevent or detect fraud, including management override of controls;
  ◦ Evaluate controls over the period-end financial reporting process;
  ◦ Scale the assessment based on the size and complexity of the company;
  ◦ Rely on management’s work based on factors such as competency, objectivity, and risk;
  ◦ Conclude on the adequacy of internal control over financial reporting.

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components.

- **Internal Environment** – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity’s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.

- **Objective Setting** –

- **Event Identification** – Internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities.

- **Risk Assessment** – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.

- **Risk Response** – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity’s risk tolerances and risk appetite.

- **Control Activities** – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.

- **Information and Communication** – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.

- **Monitoring** – The entirety of enterprise risk management is monitored and modifications made as necessary.

---

Most organizations rely on multiple sources for answers. However, risk oversight and an integrated approach is usually lacking.

**Finance**
- Internal Control, Disclosure, Credit, Liquidity, Commodity, Risk Analytics & Modeling

**General Counsel**
- Legal and Intellectual Property

**Compliance and Ethics**
- Ethics and Business Conduct, and Regulatory Compliance Risks

**Information Management**
- IT Security, Data Integrity, Information Adequacy, Business Process/Continuity Risks

**Internal Audit**
- Risk informed audits, risks to internal control, key exposures and vulnerabilities, and assurance

**Business Development**
- Market and Strategy Risks

**Security**
- Risks to property and people

**Insurance**
- Property, Casualty, Liability, and Hazards

Integrated process provides a means to better understand, communicate and respond to the risk knowledge that exists in the organization.
Risk Ranking and Prioritizing Risks (example)

- Likelihood of Occurrence
  1 = Improbable
  2 = Remote
  3 = Occasional
  4 = Frequently
  5 = All the time

- Impact of Occurrence
  1 = Minimal/Negligible
  2 = Slight
  3 = Moderate
  4 = Critical/Serious
  5 = Catastrophic

Prioritize your risks -- define your criteria first and then rank high, medium, low

<table>
<thead>
<tr>
<th>Reputation</th>
<th>Legal/Regulatory</th>
<th>Financial</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Systemic loss of public/client 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>Moderate</td>
<td>Loss of confidence among a 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>Low</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>

Significant financial impact with widespread liability

Considerable financial impact with regional liability

Minimal financial impact with localized liability
Risk Ranking and Prioritizing Risks (example)