RISK MANAGEMENT - CORPORATE COMPLIANCE & ETHICS

Presenter
CLAIRES GOMEZ-MILLER CIA CRMA FCCA CA
BOARD DIRECTOR/AUDIT COMMITTEE MEMBER
UNITED INDEPENDENT PETROLEUM MARKETING COMPANY LIMITED
TRINIDAD AND TOBAGO

RISK MANAGEMENT - CORPORATE COMPLIANCE & ETHICS

VISION – “To be the Trusted Brand for the Public’s Fuel, Automotive and Convenience Needs”
MISSION – “To offer U the Ultimate Customer Experience”
UNIPET CUSTOMERS include
- Petroleum and Compressed Natural Gas (CNG) Users.
- Private and public sector individuals and organizations - UNIPET has thousands of customers who visit its network of 24 stations every day to purchase fuel for their vehicles.
- Petroleum Dealers;
- Utilities and Energy Sector including international oil companies;
- Land based Oil Rigs;
- Marine Vessels that operate within the waters of Trinidad.
UNIPET’S use of Technology extends to the UNIPET PREPAID FLEET CARD
- Allows companies to control and manage the fuel consumed by their drivers.
- Enables individuals to be “financially ready” and to track Vehicle Maintenance and Service Schedules.
### RISK MANAGEMENT – CORPORATE COMPLIANCE & ETHICS

#### OBJECTIVE & ACKNOWLEDGEMENTS

- Risk Management is critical to the sustainability, profitability and stakeholders/public trust; to this end all organizations must demonstrate strong risk management practices.
- In the Utilities and Energy sector, risks are always very high and most likely to materialize, with heavy financial losses, lost lives and loss of operating licenses.
- Given the high expectations of all stakeholders for strong compliance and ethics, this presentation will provide participants with the latest risk management controls and emerging risks to ensure they are best prepared for when these risks materialize.

#### ACKNOWLEDGEMENTS:
- The Institute of Internal Auditors Global (The IIA) “International Standards for the Professional Practice of Internal Auditing”
- The IIA is the governing body and standard setter for internal auditors global.

### RISK MANAGEMENT – CORPORATE COMPLIANCE & ETHICS

#### AGENDA

1. Defining Risk Management & Controls
2. Meeting Stakeholders’ Expectations for Corporate Compliance, Ethics and Emerging Risks
3. Sustainability & Public Trust - Retaining your License To Operate through Effective Risks Management
4. Effective Risk Management & Controls - from Cradle to Grave to Resurrection
5. Internal Auditing – 100% Focus on Risk Management, Controls & Governance
1.1) DEFINING RISK MANAGEMENT & CONTROLS *(THE IIA)*

- Risk is “the POSSIBILITY OF AN EVENT OCCURRING that will have an IMPACT ON THE ACHIEVEMENT OF OBJECTIVES” (Institute of Internal Auditors Global).
- Risk is ANY EVENT or ACTION that PREVENTS A COMPANY FROM ACHIEVING ITS OBJECTIVES.
  - Includes Uncertain Future Events & Missed Opportunities
  - Influences achievement of Strategic, Operational, & Financial Objectives
  - Impacts Reputation and Legitimacy (License to Operate)
- Risk is measured in terms of IMPACT and LIKELIHOOD.
- RESIDUAL RISK is the risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.
- RISK APPETITE is the level of risk that an organization is willing to accept.
- RISK MANAGEMENT IS A PROCESS TO IDENTIFY, ASSESS, MANAGE, AND CONTROL potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives.

---

1.2) DEFINING RISK MANAGEMENT & CONTROLS

- ADEQUATE CONTROL - Present if management has planned and organized (designed) in a manner that provides reasonable assurance that the organization’s risks have been managed effectively and that the organization’s goals and objectives will be achieved efficiently and economically.
- CONTROL - Any action taken by Mgmt, Board, & other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
- CONTROL ENVIRONMENT - The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:
  - Integrity & ethical values. - Mgmt.'s philosophy and operating style.
  - Organizational structure. - Assignment of authority & responsibility.
  - Competence of personnel - Human resource policies & practices.
- CONTROL PROCESSES - The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.
2.1) MEETING STAKEHOLDERS' EXPECTATIONS — A BALANCED SCORECARD PERSPECTIVE

<table>
<thead>
<tr>
<th>#</th>
<th>PERSPECTIVE</th>
<th>GENERAL BUSINESS OBJECTIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stakeholder</td>
<td>To safeguard COMPANY ASSETS, REPUTATION &amp; SHAREHOLDER INVESTMENT/VALUE</td>
</tr>
<tr>
<td>2</td>
<td>Stakeholder</td>
<td>To comply with applicable LAWS, REGULATIONS AND CONTRACTS</td>
</tr>
<tr>
<td>3</td>
<td>Financial</td>
<td>To ensure SUSTAINABILITY, PROFITABILITY &amp; REVENUE GROWTH</td>
</tr>
<tr>
<td>4</td>
<td>Customer</td>
<td>To provide QUALITY GOODS, WORKS &amp; SERVICES</td>
</tr>
<tr>
<td>5</td>
<td>Customer</td>
<td>To maintain CUSTOMER SATISFACTION</td>
</tr>
<tr>
<td>6</td>
<td>Internal</td>
<td>To have SAFE, EFFECTIVE AND EFFICIENT Operations, Leadership &amp; Governance</td>
</tr>
<tr>
<td>7</td>
<td>Internal</td>
<td>To produce reliable financial &amp; operational INFORMATION, REPORTS &amp; DISCLOSURES</td>
</tr>
<tr>
<td>8</td>
<td>Learning &amp; Growth</td>
<td>To have ETHICAL, COMPETENT &amp; KNOWLEDGEABLE Directors &amp; Personnel.</td>
</tr>
</tbody>
</table>

2.2 MEETING STAKEHOLDERS' EXPECTATIONS FOR CORPORATE COMPLIANCE, ETHICS & EMERGING RISKS

They may look FAMILIAR, but they are CONTINUOUSLY EVOLVING:

- **Legal and Regulatory Requirements**
  - Integrity in Public Life & Procurement Regulations (transparent operating procedures especially in Procurement matters)
  - Anti-Corruption & Bribery
  - Anti-Money Laundering, Anti-Terrorism & Proceeds of Crime (Financial Integrity Unit)

- **Business Rules Reformation**
  - Financial Reporting & Disclosures — Transparency & Accountability
  - Extractive Industry Transparency Initiative (EITI)
  - Stock Exchange Regulations
2.3 MEETING STAKEHOLDERS’ EXPECTATIONS FOR CORPORATE COMPLIANCE, ETHICS & EMERGING RISKS

- Government Policies & Operation Style {external}
- Government Philosophy - Governance, Management and Operations {internal}
- Political Climate
- Licensing Process
- Onerous Regulatory Environment
- Information & Communication Technology
- General Infrastructure & Logistics
- Climate Change
- Culture & Language
- “Temperature” of the People
- Human Resource

2.4 MEETING STAKEHOLDERS’ EXPECTATIONS FOR CORPORATE COMPLIANCE, ETHICS & EMERGING RISKS

- Due Diligence Review – new business, market, product or partner.
- Return on Investment - Value for Money; Payback-Period, Government Involvement; legal & regulatory costs; Asset Impairment.
- Joint Ventures, Mergers & Acquisition
  - Joint Shareholder Agreement; Corporate culture;
  - Distribution of responsibilities; - Right to Audit ‘Clause;
  - Non-Operators Rights & Liabilities;
  - Operator’s Obligations, Duty of Care & Diligence.
- Financial Distress
  - Liquidity & Currency/ Foreign Exchange
  - Shareholder Demands [Dividends vs Capital Gains];
  - Take or Pay contracts; Onerous Contracts
- Loss of Capital Asset
  - Business Disruption or Abandonment {Man-made or Natural Disaster}
  - Discontinuity of Related Business
  - Nationalization of Private Assets; Privatization of State Enterprise.
3) **SUSTAINABILITY & PUBLIC TRUST - RETAINING ‘LICENSE TO OPERATE’ THROUGH EFFECTIVE RISK MANAGEMENT**

- **Occupational Safety and Health and Environmental Management**
  - Suitable and Sufficient OSH Risk Assessments & Controls
  - National Environmental Policy
  - Environmental Impact Assessments & Certificate of Environmental Clearance (CEC)
  - Inherited Environmental Risks & Provision for Abandonment
  - ISO 14000 Environmental Management System Standards

- **Federal Laws**
  - Foreign Account Tax Compliance Act (FATCA); Proceeds of Crime Act

- **Corporate Social Responsibility & Other Obligations**
  - Local Content - Minimum Wage
  - Consumer Protection - Taxations & Royalties
  - Credit Rating Agencies - Loan Covenants

---

4.1) **EFFECTIVE RISK MANAGEMENT & CONTROLS – FROM CRADLE TO GRAVE TO RESURRECTION**

To effectively manage risk, **EACH RISK**
- Must be **identified and assessed** using a TOP-DOWN APPROACH (i.e Strategic Objectives, then General Business Objectives and then down to Tactical Objectives);
- Must be **considered holistically** using a BOTTOM-UP APPROACH (i.e each Business Unit’s risk must filter up into the ERM Corporate Risk Register).
- Must have an **OWNER** (Policy Setter) and **SINGLE POINT ACCOUNTABILITY** (person responsible for ensuring execution).

- **ERM must include identification & assessment of ALL RISKS.**
- **Must have CLEAR, CONSISTENT AND SHARED** understanding of the Organization’s
  - Risk Appetite/Risk Tolerance Thresholds;
  - Risk Terminology, especially for IMPACT/SEVERITY & PROBABILITY/LIKELYHOOD
  - Risk Reporting Framework/Risk Ranking Matrix {Unacceptable/Critical /Materializing}
### 4.2a) IMPACT/SEVERITY THRESHOLD LEVELS

<table>
<thead>
<tr>
<th>RANKING</th>
<th>IMPACT/SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HIGH</strong> {7-9}</td>
<td>SAFETY &amp; ENVIRONMENT – Fatal/Extensive damage to Life/Environment (i.e., Loss of life; Group/extensive injury requiring hospitalization; Hospitalization &gt;7 Days; permanently maimed; Lost Time Incidents &gt;7 Days; involves National/ International catastrophe; long-lasting/unrecoverable damage); or REGULATORY – Imprisonment/severe long-lasting penalties (i.e., Involves failure to meet OSHA &amp; other legal &amp; statutory requirements, mission-critical contracts &amp; permits, loan covenants, national or professional regulatory standards; criminal investigation); or FINANCIAL – &gt;$50M; or REPUTATION – Serious effect on public image/stakeholder relationship (i.e., effect lasts for a sustained period or is enduring; reaches national or international media or Parliament; involves Board or high level management; difficult to erase).</td>
</tr>
<tr>
<td><strong>MEDIUM</strong> {4-6}</td>
<td>SAFETY &amp; ENVIRONMENT – Serious injury/disability/damage to environment; (i.e., long term injury/illness; Medical treatment requiring hospitalization 3-7 Days; LTI 4-7 Days; environmental disaster not easily remedied); or REGULATORY – Major Penalties, Claims &amp; Fines (i.e., Criminal/Integrity Probe; involves failure to meet non-mission critical contracts, shareholder mandates, board policies, industrial standards); or FINANCIAL – $25M - $50M; or REPUTATION – Significant effect on public image/stakeholder relationship (i.e., effect can be counteracted; reaches the press but there is quick response; some long-lasting residual effects).</td>
</tr>
<tr>
<td><strong>LOW</strong> {1-3}</td>
<td>SAFETY &amp; ENVIRONMENT – Minor impact on person/environment (i.e., minor injury requiring First Aid treatment; Loss Time Incidents &lt;1-3 Days; Hospitalization for observation/treatment &lt;3 Days); or REGULATORY – Minor penalties (i.e., involves failure to meet Reporting Requirements &amp; Best Practices (i.e., involves failure to meet Stakeholder/Civil Society Expectations; short-term effects); or FINANCIAL – &lt;$25M; or REPUTATION – Little or no effect on public image/stakeholder relationship (i.e., reaches the press/public but it affords quick response; negative impression can be erased with little or no residual effects).</td>
</tr>
</tbody>
</table>

CGM 22FEB2015

SCCE Utilities & Energy Conference 2015, Houston TX
### 4.2c) PROBABILITY/ LIKELIHOOD THRESHOLD LEVELS

<table>
<thead>
<tr>
<th>High {7-9}</th>
<th>Medium {4-6}</th>
<th>Low {1-3}</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely to occur. The event occurs once or more per year; frequent occurrence.</td>
<td>Likely to occur Event occurs once or more every 5 years; Occasional.</td>
<td>Unlikely to occur Event occurs outside of 5 years; Rare occurrence.</td>
</tr>
</tbody>
</table>

### 4.2d) RISK TREATMENT

<table>
<thead>
<tr>
<th>INHERENT RISKS</th>
<th>RESIDUAL RISKS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Accept (If within preset criteria)</td>
<td>Retain</td>
<td>Insurable</td>
</tr>
<tr>
<td>• Reduce/Prevent;</td>
<td>• Required to be Retained</td>
<td>Or</td>
</tr>
<tr>
<td>• Share (i.e., Transfer in Part)</td>
<td>• Avoid: Proceed using less risky alternative.</td>
<td>Not</td>
</tr>
<tr>
<td>• Transfer in Full</td>
<td>• Avoid: Do not proceed with Activity</td>
<td>Insurable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not insure</td>
</tr>
</tbody>
</table>

### 4.2e) ERM - CORPORATE RISK RANKING MATRIX

<table>
<thead>
<tr>
<th>MAJOR (HIGH IMPACT / LOW LIKE'D)</th>
<th>CRITICAL (HIGH IMPACT / MED LIKE'D)</th>
<th>UNACCEPTABLE (HIGH IMPACT / HIGH LIKE'D)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH IMPACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9 18 27</td>
<td>9 18 27 36 45 54 63 73 81</td>
</tr>
<tr>
<td>8</td>
<td>8 16 24</td>
<td>8 16 24 32 40 48 56 64 72</td>
</tr>
<tr>
<td>7</td>
<td>7 14 21</td>
<td>7 14 21 28 35 42 49 56 63</td>
</tr>
<tr>
<td>MED IMPACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6 12 18</td>
<td>6 12 18 24 30 36 42 48 54 63</td>
</tr>
<tr>
<td>5</td>
<td>5 10 15</td>
<td>5 10 15 20 25 30 35 40 45</td>
</tr>
<tr>
<td>4</td>
<td>4 8 12</td>
<td>4 8 12 16 20 24 28 32 36</td>
</tr>
<tr>
<td>LOW IMPACT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3 6 9</td>
<td>3 6 9 12 15 18 21 24 27</td>
</tr>
<tr>
<td>2</td>
<td>2 4 6</td>
<td>2 4 6 8 10 12 14 16 18</td>
</tr>
<tr>
<td>1</td>
<td>1 2 3</td>
<td>1 2 3 4 5 6 7 8 9</td>
</tr>
<tr>
<td>LOW LIKEL'D</td>
<td>MED LIKEL'D</td>
<td>HIGH LIKEL'D</td>
</tr>
</tbody>
</table>
4.3) EFFECTIVE RISK MANAGEMENT & CONTROLS – FROM CRADLE TO GRAVE TO RESURRECTION

To effectively manage risk, EACH RISK

- must be consistently managed FROM CRADLE TO GRAVE TO RESURRECTION.

  - For EACH GENERAL BUSINESS AND STRATEGIC OBJECTIVE
    - What will prevent me from achieving my Objective?

  - From INHERENT RISK STAGE
    - If I don’t manage this risk, what is the Potential Impact – Safety & Environmental? Regulatory? Financial? Reputation?
    - And what is the Likelihood?

  - Down to RESIDUAL RISK STAGE
    - Managed State, after mitigating measures & controls
    - If still unacceptable, then seek to insure the residual risk.

  - To RISK MATERIALIZATION STAGE
    - Response – what must I do when the risk materializes?

  - And RECOVERY
    - Business Continuity – what must I do to restart my business process/operations?

4.4) EFFECTIVE RISK MANAGEMENT – FROM CRADLE TO GRAVE TO RESURRECTION

AN EXAMPLE

ENTERPRISE RISK MANAGEMENT - SPECIMEN.pdf

CGM 22FEB2015 SCCE Utilities & Energy Conference 2015, Houston TX 18
7) INTERNAL AUDITING: 100% FOCUS ON RISK MANAGEMENT, CONTROLS & GOVERNANCE

IIA DEFINITION: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization achieve its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

NATURE OF WORK - Internal Auditors MUST

- Evaluate the RISK EXPOSURES and the ADEQUACY AND EFFECTIVENESS OF CONTROLS IN RESPONDING TO RISKS within the organization's governance, operations, and information systems regarding the:
  - Achievement of the organization's strategic objectives
  - Reliability and integrity of financial & operational information;
  - Effectiveness and efficiency of operations;
  - Safeguarding of assets; and
  - Compliance with laws, regulations, and contracts.
- Promote appropriate ethics and values within the organization;
- Ensure effective organizational performance management and accountability;
- Communicate risk and control information to appropriate areas of the organization; and
- Coordinate the activities of and communicate information among the board, external and internal auditors, and management.