Enterprise Risk & Governance

April 2013
The Suncor Operations Excellence Management Systems (OEMS)

- Developed to provide a framework for company policies, standards, and procedures to support the company’s goal of operational excellence
- Lays out the requirements / expectations for the management of operational risks inherent in Suncor’s businesses
- The OEMS contains the requirements for the development and sustainment of an effective risk and hazard identification process and effective processes to mitigate said risks
- The OEMS also lays out requirements for the governance of the OEMS itself, and supporting programs, risks and controls in the areas of Health, Environment, Personal and Process Safety, Wellness, Security etc which fall under its scope.

The following slides provide an overview of Suncor’s approach to risk management and governance, focusing in particular on the role of the Corporate Operations Integrity Audit function.
Overview of Suncor Operations Excellence
MS Structure

1. Leadership, Integrity & Accountability
2. Risk Identification, Assessment & Management
3. Legal Requirements & Commitments
4. Objectives, Targets and Planning
5. Management of Change
6. Structure, Responsibility & Resources
7. Training & Competence
8. Facilities Design & Construction
9. Operations & Maintenance Controls
10. Contractor Management & Third Party Services
11. Data & Document Management
12. Emergency Preparedness & Response
13. Information & Communication Management
14. Quality Assurance
15. Incident Reporting, Investigation & Learning
16. Operations Integrity Monitoring, Audit & Assessment
17. Corrective & Preventative Action
18. Stewardship & Management Review
Operational Excellence Management System

**Why**
- Strategy
- Values
- Policies

**What**
- Business Processes
- Standards & Guidelines*
- Procedures, Work Practices and Tools

**How**
- Individual Actions

* Includes process safety management standards

**Operational Excellence Management System**

- Company-wide

**Business Processes**

- Company-wide, BU / FN

**Standards & Guidelines***

- Company-wide, BU / FN

**Procedures, Work Practices and Tools**

- Company-wide, BU / FN, Facility/site specific

**What**
- Requirements of the business to manage operational risks, mitigate environmental impacts and deliver safe, reliable operations
- Steps that outline interrelated activities that require resources and turn inputs into clearly defined outputs
- Performance expectations to demonstrate compliance with OEMS requirements, including process safety management
- Procedures, practices and tools that operationalize the management system

**HOW**
- Demonstrated behaviours that minimize risk to self, others, the environment, assets and stakeholders

* Includes process safety management standards
Long Term Benefits of OEMS Governance Initiatives -- Operational Excellence

- Process for the continual reduction of Suncor risk profile, and in particular those low probability but high consequence events that have been occurring with increased frequency in our industry over the last few years
- Improved operational discipline, and corresponding improvements in asset reliability and production performance
- Identification of controls weakness and/or continual improvement opportunity
- Improved regulatory compliance controls, and resultant stakeholder relations
- Risk transparency
- Facilitates achievement of stretch environmental Goals
Operations Integrity Audit

- The Director of the Operations Integrity Audit group reports directly to the Chair of the EHS SD Committee to maintain third party independence
- 2$ Million dollar budget
- 6 full time professional auditors
- Pool of 80 qualified auditors to draw on from operations, as well as usage of external experts
- Works closely with Internal Audit and conducts joint audits where required
- 70 auditable units across the company
- Conducts 30 plus assessments per year
- Trains auditors, and develops audit protocols and auditor guidance for all key requirements
- Maintains common audit software platform, and analyses incident and audit data for trends and emerging risks

- As a requirement of the Operations Excellence management System and Process Safety Management Business Units are required to develop quality risk registries and legal registries, and to use the data in business planning
- A common risk matrix is used across the company and all risk data will be entered into a common company wide data base in 2011
- Business units are required to develop a 3 year risk based schedule of 1st, 2nd and 3rd party audits to demonstrate level 1 and 2 risk controls effectiveness and regulatory compliance, taking into account their principal risks, incident history, previous audit findings, etc
- Business Units are required to conduct annual self assessments against all 18 elements of the Operations Excellence Management System and all 14 Process Safety Management program elements over a 3 year cycle
- The OEMS and PSM peer networks and element leads participate in and provide a quality assurance to the conduct of the self assessment program, as well as facilitating the sharing of best practices across Suncor
Operations Integrity Audit

- Operations Integrity Audit is required to manage a fixed cycle of 3 year third party audits for the Suncor Operations Excellence Management System and Process Safety Management program to validate the findings of the self assessment programs.

- Operations Integrity Audit undertakes additional risk based audits (taking into account those risks and controls that Operations has indicated they will assess directly).

- All Operations Integrity Audit findings are analyzed and tracked and unacceptable level 1 risk findings are escalated to the EHS SD Board Committee.

- The EHS SD Committee reviews the EHS SD stewardship data and audit findings on a quarterly basis and makes recommendations on strategic EHS SD goals and initiatives and those critical risks for which they would like third party validation of control effectiveness.
The Risk Management Process
Risk Assessment Model (Adapted from Standard AS/NZS 4360:2004)
OEMS Element 2 and related PS Standard requirements

Strategic Process
(Framework continuous improvement cycle)

Mandate & Commitment
Policy Standards Procedures/Guidelines

Communicate & Train
Communication Reporting Training

Risk Structure & Accountability
Risk Roles & Responsibilities:
Executive Leadership Team Chief Risk Officer Business & Function Leaders & Management

Communicate and consult

1. Establish the context
2. Risk assessment
   2a.
   2b.
   2c.
3. Treat risks
4. Monitor and review

Process for Managing Risk

Measure, Review & Improve
Control Assurance Policy Standards & Guidelines KPIs KRIIs

Risk management information to action
- Risk Assurance - Risk Registers
- Treatment Plan - Reporting Templates

Strategic Process
(Framework continuous improvement cycle)
Suncor Risk Matrix

<table>
<thead>
<tr>
<th>Likelihood Category - Frequency Guidelines (Business Unit Basis)</th>
<th>Event Description</th>
<th>Project Evaluation Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>f ≥ 1 yr</td>
<td>Causes once per year in BU without any injuries or fatalities</td>
<td>Higher than 95% chance</td>
<td>Probable</td>
</tr>
<tr>
<td>8.1 x f ≤ 1 yr (between 1 year and 10 years)</td>
<td>Expected to occur several times in the Buitread, lifetime</td>
<td>75% - 90% chance</td>
<td>Possible</td>
</tr>
<tr>
<td>0.61 x f ≤ 0.1 yr (between 1/10 and 1/100 years)</td>
<td>Expected to occur in the Buitread lifetime</td>
<td>55% - 70% chance</td>
<td>Unlikely</td>
</tr>
<tr>
<td>0.01 x f ≤ 0.01 yr (between 1/100 and 1/1000 years)</td>
<td>May happen less than once during the Buitread lifetime</td>
<td>30% - 50% chance</td>
<td>Remote</td>
</tr>
<tr>
<td>0.1 x f ≤ 0.001 yr (between 1/1000 and 1/10000 years)</td>
<td>Remote chance of happening</td>
<td>10% - 30% chance</td>
<td>Remote</td>
</tr>
<tr>
<td>f &lt; 0.0001yr (less than 1/10,000 years)</td>
<td>Extremely remote chance of happening</td>
<td>Less than 10% chance</td>
<td>Extremely Remote</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequence Category</th>
<th>Increasing Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>C2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action Priorities</th>
<th>Residual Risk Level</th>
<th>Risk Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>I</td>
<td>Responsible Senior Leader in BU is made aware of risks and mitigation plans are implemented</td>
</tr>
<tr>
<td>II</td>
<td>II</td>
<td>Responsible VP ensures preventive controls and mitigation plans are established and maintained and risks are reassessed at appropriate intervals</td>
</tr>
<tr>
<td>III</td>
<td>III</td>
<td>Line management monitors the risks, ensures operational controls and mitigation plans are functioning, and procedures are followed</td>
</tr>
<tr>
<td>IV</td>
<td>IV</td>
<td>Front line leaders ensure that employees and contractors are aware of the risk, and follow established procedures and operational controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Social</th>
<th>Health &amp; Safety (Public and Employees)</th>
<th>Incident: no treatment</th>
<th>Single restricted work site or medical facilities</th>
<th>Single restricted work site or medical facilities</th>
<th>Single restricted work site or medical facilities</th>
<th>Single restricted work site or medical facilities</th>
<th>Single permanent disability or multiple lost time cases</th>
<th>Fatality or multiple fatality disabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reputations (legal requirements &amp; commitments)</td>
<td>Individual concern - single stakeholder complaint</td>
<td>No impact</td>
<td>No impact</td>
<td>No impact</td>
<td>No impact</td>
<td>No impact</td>
<td>No impact</td>
</tr>
<tr>
<td></td>
<td>Regulatory Consequence</td>
<td>Below regulatory limits</td>
<td>Regulatory notification required</td>
<td>Regulatory notification required</td>
<td>Regulatory notification required</td>
<td>Regulatory notification required</td>
<td>Regulatory notification required</td>
<td>Regulatory notification required</td>
</tr>
<tr>
<td></td>
<td>Environmental Consequence</td>
<td>Release to on-site environment, controlled</td>
<td>Release to on-site environment, controlled</td>
<td>Release to on-site environment, controlled</td>
<td>Release to on-site environment, controlled</td>
<td>Release to on-site environment, controlled</td>
<td>Release to on-site environment, controlled</td>
<td>Release to on-site environment, controlled</td>
</tr>
<tr>
<td></td>
<td>Economic Consequence</td>
<td>Business Operating Costs</td>
<td>$100k &lt; C &lt; $1M</td>
<td>$1M &lt; C &lt; $10M</td>
<td>$10M &lt; C &lt; $100M</td>
<td>$100M &lt; C &lt; $500M</td>
<td>C &gt; $500M</td>
<td>C &gt; $500M</td>
</tr>
<tr>
<td></td>
<td>Project Costs</td>
<td>% of total Project</td>
<td>1% &lt; C &lt; 3%</td>
<td>3% &lt; C &lt; 6%</td>
<td>6% &lt; C &lt; 9%</td>
<td>9% &lt; C</td>
<td>C &gt; 9%</td>
<td></td>
</tr>
</tbody>
</table>

Authorized 2 February 2010, Suncor Energy BOD meeting

UNCONTROLLED DOCUMENT WHEN PRINTED

SUNCOR ENERGY
Suncor Risk Registries

Suncor Principal Risk Registry

Suncor Corporate Risk Registry

Other BU Risk Registries

Business Area A Risk Registry

Business Area B Risk Registry

Business Area C Risk Registry

Business Unit Principal Risk Registry

Prioritized BU Risks

Business Unit Risk Registry

BA A+B+C Risks

Additional BU Risks

Unit 1 Risk Registry

Unit 2 Risk Registry

Unit 3 Risk Registry

PHA Hazops, LOPAs, What Ifs

PHA Hazops, LOPAs, What Ifs

PHA Hazops, LOPAs, What Ifs

Other BU Risk Registries

Other BU Risk Registries

Other BU Risk Registries

Suncor Corporate Risk Registry

Suncor Principal Risk Registry

Suncor Risk Registries
Operating Businesses

ERM

OEMS

Internal Audit

Operations Integrity Audit

- Building top-down / bottom up risk inventories
- Alignment with OEMS Element No 2
- Risk Management Standards & Tools
- Challenges: pace of maturity is dependant on Business Readiness and Culture

- Audit Plan integration
- Consistency in use of risk taxonomy, risk universe, risk matrix and "bow-tie" risk analysis
- Challenges: risk inventories is not fully mature

- Joint audit planning & coordination
- Joint audits for end-to-end processes and cross-boundary risks
- Tracking and follow-up reporting
- Quarterly team meetings
- Challenges: Reporting is not fully aligned; audit staff integration

- Program expertise
- Base-line assessment
- Challenges: Capacity within operating businesses

Overall governance model is organized well for providing risk assurance. Execution challenges will require leadership drive and business unit maturity on Enterprise Risk Management (ERM) and Operations Excellence Management Systems (OEMS).
**Principle Risk Registry for a Hypothetical Oil Sands Operation**

<table>
<thead>
<tr>
<th>Likelihood Category</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>C5</th>
<th>C6</th>
</tr>
</thead>
<tbody>
<tr>
<td>L6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Likelihood Category

- **L6**: Virtually certain
- **L5**: Probable
- **L4**: Possible
- **L3**: Unlikely
- **L2**: Rare
- **L1**: Remote

### Consequence Category

- **C1**: <$100K
- **C2**: $100K to <$1M
- **C3**: $1M to <$10M
- **C4**: $10M to <$100M
- **C5**: $100M to <$500M
- **C6**: >$500M

### Consequence Category

- **Environmental Policy / Regulation Change**
- **Permit Approval Risk**
- **Natural Disaster / Business Continuity Planning**
- **Protracted Operational Outage**
- **EH&S / Regulation Non-Compliance**
- **Sil & Resource Shortage**

### Notes:

- Based on risk assessment for YE 2008 for legacy SU and legacy PC
- Identified as a principal risk for legacy Suncor
Enterprise risk Management

- Principle risks in each area are reviewed at least annually, looking at pure risk and mitigated risk rating taking into account the operational controls used to manage the risk.

- These controls are often the focus of self assessments, 2nd party and 3rd party audits to validate their effectiveness.

- Operational Risks are also identified from the bottom up, with legal and other requirement registries and risk registries part of the OEMS.

- These registries (which include environmental risks) are based on professional judgment, hazops, PHAs, and other hazard and risk identification methodology.

- All level 1 and 2 risks must be managed by the affected leadership team.

- Intent over longer term is that Company wide risk data will be entered and managed in one software tool to facilitate analysis and trending of lower level risks.
Risk Management Maturity Road Map

- **LEVEL 1**
  - Unaware of the need for risk management
  - No structured approach to dealing with uncertainty, resulting in a series of crises for each project or operation

- **LEVEL 2**
  - No formal or structured Risk Management process in place
  - Organization is aware of potential benefits of managing their project risks
  - No effectively organization-wide process implemented

- **LEVEL 3**
  - Implemented risk management into routine business processes
  - Implements risk management in most, if not all, projects

- **LEVEL 4**
  - Established a risk-aware culture that requires a proactive approach to the management of risks in all aspects of the organization

*Journey to Zero*
OPERATIONAL EXCELLENCE

every day, a better way