

# ENTERPRISE RISK MANAGEMENT



**FACC 6300.C: RISK GOVERNANCE (LECTURE #2)**  
© 2019. Ingrid Robinson



*Ingrid Robinson, MFAc, BComm, CPA, CIA, CRMA*

# **KEY LEARNINGS: LECTURE #1**

# AGENDA

- **Regulatory Landscape**
- **Risk Oversight: Board's Role**
- **Risk Governance Framework**
- **BREAK (8:45pm; 15 minutes)**
- **Case Study: China Aviation Oil Corporation**

# REGULATORY LANDSCAPE

RISK OVERSIGHT RULES



# WHAT IS CORPORATE GOVERNANCE?

- **Process/structure** to direct and manage the business and affairs of the firm
- Defines the **division of responsibility** and establishes mechanisms for achieving accountability among stakeholders, the Board of Directors and management
- Objective is to **enhance stakeholder value** while properly discharging fiduciary duties

# FINANCIAL CRISIS: BOARD OVERSIGHT FAILURE



*“The greatest tragedy would be to accept the refrain that no one could have seen this coming and thus find nothing could have been done. If we accept this notion, it will happen again”*

*[Financial Crisis Inquiry Commission]*



# FINANCIAL CRISIS: WHAT HAPPENED...

## ■ Conditions triggered economic downward spiral:

- ✓ Sub-prime meltdown
- ✓ Liquidity crisis
- ✓ Extreme market volatility

## ■ Repercussions spread to broader economy:

- ✓ Global credit market constriction
- ✓ Reduced consumer demand
- ✓ Volatile commodity prices, currencies and stock prices



# FINANCIAL CRISIS: WHY IT HAPPENED...

- **Lack of integration between strategy and risk management**
- **Compensation programs conflicted with the objectives of the firm**
- **Fragmented technology infrastructures hindered effective risk identification/measurement**
- **Ineffective risk reporting**
- **Undue risk taking led to financial instability**



# FINANCIAL CRISIS: WHY IT HAPPENED...

- **Fragmented risk oversight responsibilities**
- **Inconsistent governance structures (Board and management)**
- **Insufficient risk experience among Board members**
- **Inadequate Board oversight of risk**



*“While risk management is the responsibility of Executives, it is incumbent on the Board to put in place the governance controls that ensure that risk management processes are adequate and effective.” (Alles and Friedland, 2010)*

# RISK OVERSIGHT: A BOARD PRIORITY

**July 2010 Dodd-Frank signed into law...requires that a Board risk committee be established by all public bank holding companies (and non-bank financial institutions supervised by the Federal Reserve) with over \$10 billion in assets.**

**COSO surveyed 200 corporate directors on the current and desired future state of risk oversight applied by Boards. 53% rated risk oversight as effective or highly effective. 70% indicated their Boards are NOT formally executing mature/robust risk oversight”**  
**(The Pak Banker. Lahore: December 2010)**



**Boards are “re-examining governance structure and roles, risk policies and limits, and assurance and reporting processes”.**  
**(J. Lam. April 2011. The RMA Journal, Vol 93, Iss. 7:51)**

# RISK GOVERNANCE LANDSCAPE

**Public and political perception that undue risk-taking was central to the financial crisis triggered an avalanche of legislative, regulatory, and judicial reform on risk management and risk prevention**



# GLOBAL RISK GOVERNANCE REGULATIONS



NP 58-201 (2005)



303.09A (2010)



UK Corporate  
Governance Code  
(2010)



Corporate Governance  
Principle 7



Corporate Governance  
Code & Risk Governance  
Guide (2012)



Supervisory Regulations  
on Corporate Governance  
of Financial Companies



Companies Act, Sec 177  
(2013)



Law of the People's  
Republic of China on  
Securities – Article 124



Corporate Governance Code  
– Risk Management and  
Internal Control



Corporate Governance  
Code Principle 4



F R C of Nigeria  
National Code of Corporate  
Governance (2016), P. 30

# RISK GOVERNANCE LANDSCAPE

## Canada: National Policy 58-201 (2005)

- **Board should adopt mandate explicitly acknowledging responsibility for:**
  - **Adopting strategic plan that takes opportunities and risks of the business into account**
  - **Identification of principal risks, and ensuring implementation of appropriate systems to manage these risks**



# RISK GOVERNANCE LANDSCAPE

## Canada: OSFI (2012)

- **FRFI should have a Board-approved Risk Appetite Framework that guides the risk-taking activities of the FRFI**
- **Depending on the nature, size, complexity and risk profile of the FRFI, the Board should establish a dedicated Committee to oversee risk**
- **FRFIs should have a senior officer who has responsibility for the oversight of all relevant risks across the firm (CRO or equivalent), with sufficient stature, authority and independence**
- **CRO should have unfettered access and, for functional purposes, a direct reporting line to the Board or the Risk Committee**



# RISK GOVERNANCE LANDSCAPE

## US: New York Stock Exchange 303A.09 (2010)

- **Audit committee required to discuss guidelines and policies to govern the process by which risk assessment and management is undertaken**
- **Large financial institutions required to constitute independent Risk Committees**



# RISK GOVERNANCE LANDSCAPE

## US: Dodd Frank Wall Street Reform Act

- **Banks with > \$50 billion in assets, listed firms with > \$10 billion in assets and certain other non-bank systemically important financial companies must have a Risk Committee and Charter**



# RISK GOVERNANCE LANDSCAPE

## UK: Corporate Governance Code, Section 3 (2010)

### ▪ Board responsibilities:

- **Determining tolerable significant risks in achieving strategic objectives**
- **Maintaining sound risk management systems**
- **Establishing formal and transparent mechanisms for considering risk management and internal control principle application**



# RISK GOVERNANCE LANDSCAPE

## AUS: Corporate Governance Principle 7 (2010)

### ▪ Board responsibilities:

- **Committee to oversee risks and disclose Committee Charter**
- **If Committee is not in place, disclose processes employed to oversee risk management framework**
- **Review risk management framework annually**
- **Disclose risks in directors report**



# RISK GOVERNANCE LANDSCAPE

## SING: Risk Governance Guidance for Listed Boards (2012)

- **Supports integrated enterprise-wide perspective on risk management**
- **Sets Board and management responsibility for risk oversight and management**



# RISK OVERSIGHT

BOARD'S ROLE



# WHAT IS RISK GOVERNANCE?

## ■ Oversight process of the Board that:

- Establishes the structure for governing risk
- Ensures appropriate risk management systems are in place to enforce and monitor risk parameters

- Sets the parameters (“limits”) for acceptable risk taking by the organization in the pursuit of strategic objectives
- Understands major risks faced by the organization
- Provides confidence and guidance to management in its risk-based decision making



“

**COMMUNICATING WITH INVESTORS ABOUT RISK**

**According to data from the 2014-2015 National Association of Corporate Directors (NACD) Public Company Governance Survey, oversight of risk management was one of the top five issues discussed with institutional investors over the past year.**

”

**NACD ADVISORY COUNCIL ON RISK OVERSIGHT**

# IN 2019 INVESTORS EXPECT...



- 1. Clear risk oversight roles for the Board, Committees and management**
- 2. Board expertise tied to key risks**
- 3. Board oversight of key risks**
- 4. Management reporting to the Board**
- 5. Reinforcement of accountability for risk**
- 6. Defined risk appetite**
- 7. Integration of strategy, risk and performance**
- 8. Holistic definition of risks and full appreciation of significant risks**
- 9. How firms are responding to external market developments and industry trends**
- 10. Assessment of risk culture**
- 11. Contextual, transparent and dynamic risk reporting**
- 12. Assurance that mitigation has reduced risk exposure**

# BOARD RISK OVERSIGHT MANDATES

## SUN LIFE FINANCIAL

Our Board of Directors is ultimately responsible for ensuring the oversight of all risks across the enterprise and has primary responsibility for taking action to ensure risk management policies, programs and practices are in place. By approving our Risk Framework and the Risk Appetite Policy, and providing ongoing oversight of the risk management programs, the Board of Directors monitors that the principal risks are appropriately identified and managed. The Board of Directors oversees business and strategic risk through review and approval of the business and strategic plans, and regularly discusses key themes, issues and risks emerging in connection with the design or implementation of these plans. The Board of Directors also monitors risk management activities of our subsidiaries and risk posed to the Company through its joint venture arrangements.

**The Risk & Conduct Review Committee** is a standing committee of the Board of Directors whose primary functions are to assist the Board of Directors with oversight of the management of risk enterprise-wide and of the risk management function, to ensure that management has in place policies, processes and controls designed to identify and effectively manage the significant risks to which the Company is exposed and has sufficient capital to underpin those risks. The Committee regularly monitors that the risk profile is within the agreed risk appetite of the Company and that the Company's capital position is in compliance with regulatory capital requirements, and recommends to the Board for approval, and monitors, the specific risk limits allocated to the businesses and the annual Capital Plan. The Risk & Conduct Review Committee meets with senior business and functional leaders who have firsthand knowledge of risks and the risk management programs, oversees the effectiveness of the risk management function, and obtains reports from Internal Audit on the effectiveness of risk controls within the business and risk function. It reviews and approves all risk management policies and reviews compliance with those policies. In addition, where the Board of Directors has allocated oversight of specific risk management programs to other committees of the Board of Directors ("Board Committees"), the Risk & Conduct Review Committee is tasked with providing the Board of Directors with an integrated view of oversight of all risk management programs across all Board committees. The committee also oversees compliance with legal and regulatory requirements and the identification and management of compliance risk.

**The Governance, Nomination & Investment Committee** of the Board of Directors is responsible for assisting the Board of Directors in reviewing and monitoring the Company's Investment Plan and investment performance, overseeing investment practices, procedures and controls related to the management of the general fund investment portfolio and the Company's asset management businesses, and reviewing and approving transactions, either separately or jointly with the Risk & Conduct Review Committee, where the acquisition of individual investments for the General Account would, on their own, exceed certain limits or ranges in the Investment and Credit Risk Management Policy. In addition, the Committee is also responsible for developing effective corporate governance guidelines and processes including policies and processes to sustain ethical behaviour, and developing processes to assess the effectiveness of the Board of Directors and its Committees.

**The Audit Committee** of the Board of Directors is responsible for assisting the Board of Directors in overseeing the integrity of financial statements and related information provided to shareholders and others, compliance with financial regulatory requirements, adequacy and effectiveness of the internal controls implemented and maintained by management, and assessing the qualifications, independence and performance of the external auditor.

**The Management Resources Committee** of the Board of Directors is responsible for assisting the Board of Directors in ensuring we have the leadership resources for succession of senior executive positions and programs to effectively attract, retain, develop and reward executives for achieving our strategic objectives. The Management Resources Committee reviews the design, approval and governance of material incentive programs to align business objectives and incentives to ensure that these incentive programs do not encourage excessive risk taking, and reviews the implications of key enterprise risks, including human resources risks, on compensation design and human resources practices. In addition, the Management Resources Committee reviews and makes recommendations to the Board of Directors with respect to compensation matters, including the remuneration of executives who have a material impact on the risk exposure of the Company. Management's

# BOARD RISK OVERSIGHT MANDATES

## BROOKFIELD ASSET MANAGEMENT

The Corporation's Board of Directors has governance oversight for risk management with a focus on the more significant risks we face, and builds upon management's risk assessment and oversight processes. The Board of Directors has delegated responsibility for the oversight of specific risks to board committees as follows:

**Risk Management Committee:** Oversees the management of Brookfield's significant financial and non-financial risk exposures, including market, credit, operational, reputational, strategic, regulatory and business risks. These responsibilities include reviewing risk assessment and risk management practices with management to ensure ongoing, effective mitigation of key organizational risks, as well as confirming that the company has an appropriate risk taking philosophy and suitable risk capacity.

**Audit Committee:** Oversees the management of risks related to Brookfield's systems and procedures for financial reporting as well as for associated audit processes (internal and external). Part of the Audit Committee's responsibilities is the review and approval of the risk-based internal audit plan, which ensures alignment with risk management activities and organizational priorities.

**Management Resources and Compensation Committee:** Oversees the risks related to Brookfield's management resource planning, including succession planning, proposed senior management appointments, executive compensation, and the job descriptions and annual objectives of senior executives, as well as performance against those objectives.

**Governance and Nominating Committee:** Oversees the risks related to Brookfield's governance structure, including the effectiveness of board and committee activities and potential conflicts of interest, as well as with respect to related party transactions.

Brookfield

Source: Brookfield Asset Management, Annual Report, 2016, Page 70.

# BOARD RISK OVERSIGHT MANDATES

## BARRICK GOLD

The ability to deliver on our vision, strategic objectives and operating guidance depends on our ability to understand and appropriately respond to the uncertainties or “risks” we face that may prevent us from achieving our objectives. In order to achieve this we:

- Maintain a framework that ensures we manage risk effectively and in a manner that creates the greatest value;
- Integrate a process for managing risk into all our important decision-making processes so that we reduce the effect of uncertainty on achieving our objectives;
- Ensure that the key controls we rely on to achieve the Company’s objectives are actively monitored so that they remain in place and are effective at all times; and
- Provide assurance to the Executives and relevant Committees of the Board of Directors on the effectiveness of key control activities.

### **Board and Committee Oversight**

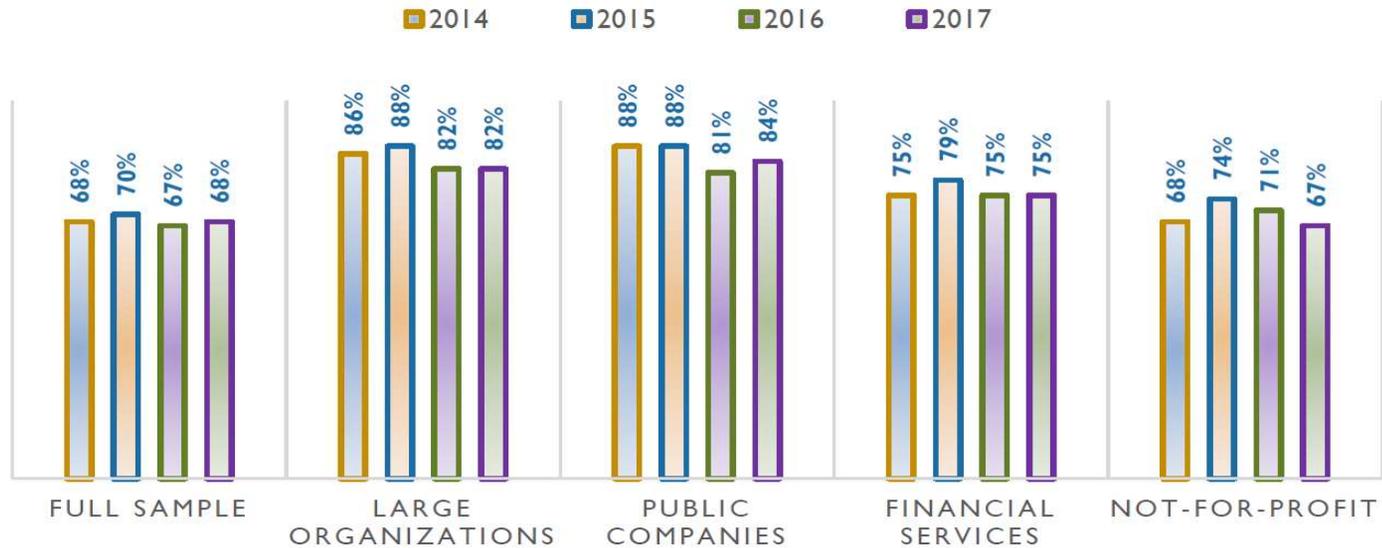
We maintain strong risk oversight practices, with responsibilities outlined in the Board’s and related committees’ mandates. The Board’s mandate makes clear the responsibility for reviewing and discussing with management the processes used to assess and manage risk, including the identification by management of the principal risks of the business, and the implementation of appropriate systems to deal with such risks.

The Risk Committee of the Board of Directors assists the Board in overseeing the Company’s management of principal risks as well as the implementation of policies and standards for monitoring and modifying such risks, and monitoring and reviewing the Company’s financial position and financial risk management programs generally. The Audit Committee and Corporate Responsibility Committee also provide oversight focusing on financial and operational (e.g. Safety & Health, Environmental, Community, Security, etc.) risk exposures, respectively.



# BOARDS ASKING FOR MORE...

EXTENT TO WHICH BOARDS ARE ASKING FOR MORE SENIOR EXECUTIVE INVOLVEMENT IN RISK MANAGEMENT  
"SOMEWHAT", "MOSTLY", OR "EXTENSIVELY"



Source: AICPA & NC State ERM Initiative. An Overview of ERM Practices. 9<sup>th</sup> Edition. March 2018

# BOARD REPORTING

PROVIDE FORMAL REPORT TO BOARD DESCRIBING TOP RISK EXPOSURES AT LEAST ANNUALLY



Source: AICPA & NC State ERM Initiative. An Overview of ERM Practices. 9<sup>th</sup> Edition. March 2018

# RISK MITIGATION DISCLOSURE

## Social license to operate

At Barrick, we are committed to building, operating, and closing our mines in a safe and responsible manner. To do this, we develop long-term and mutually-beneficial relationships with host governments and communities while working to minimize the social and environmental impacts of our activities. Incidents of **corruption** in the extractive industry are indicative of the risks related to interaction with government officials and the potential consequences to our partnerships in the locations where we operate. **Environmental incidents** in the extractive industry emphasize the hazards (e.g. water management, tailings storage facilities, etc.) and the potential consequences to both the environment and **community health and safety**. Our ability to maintain **compliance** with environmental, regulatory and community obligations remains one of our top priorities.

## Key Risk Modification Activities:

- Our external Corporate Social Responsibility Advisory Board was formed in 2012 and provides expert advice to the Company on a range of corporate responsibility matters, including community relations, sustainable development, water, energy, climate change, security and human rights;
- Our obligations, expectations and intentions are codified in our Vision and Values and the Code of Business Conduct and Ethics, and they are reinforced regularly at all levels of the Company;
- Barrick's community relations, environment, safety and health, security and compliance management systems set expectations, define performance standards and provide the necessary tools to modify the related risks;
- We take a partnership approach with our home and host governments. This means we work to balance our own interests and priorities with those of our government partners, working to ensure that everyone derives real value from our operations;
- We participate in the annual CDP Climate Change and Water Disclosure process, providing investors and other interested partners with detailed information on our water and energy use and emissions data; and
- We open our social and environmental performance to third-party scrutiny, including through the ISO 14001 re-certification process, International Cyanide Management Code audits, annual human rights impact assessments, and an annual assurance against the International Council on Mining and Metal's Sustainable Development Framework.



Source: Barrick Gold, Annual Report, 2016, Page 35-36.

# **RISK GOVERNANCE FRAMEWORK**

**LEADING PRACTICE**



# RISK GOVERNANCE FRAMEWORK

## GOVERNANCE

**Establish an effective governance structure to oversee risk**



## POLICY

**Approve/monitor risk policy**

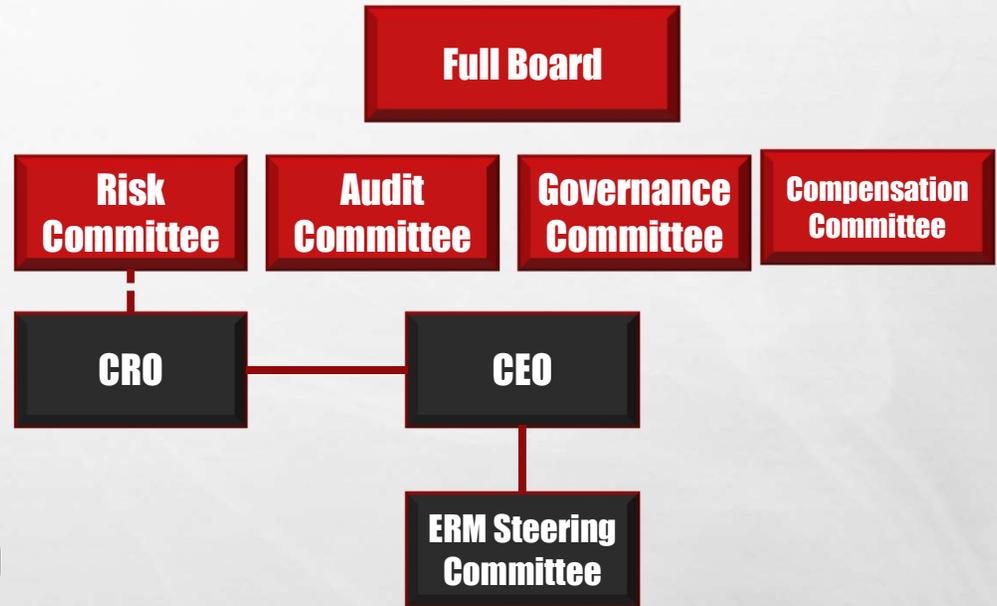


## ASSURANCE

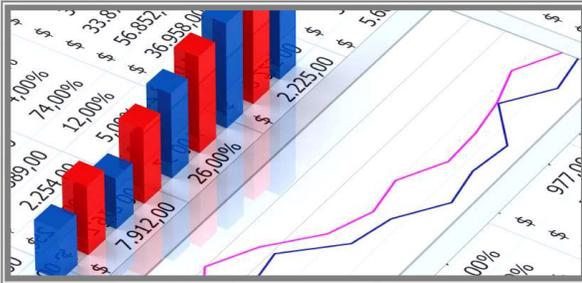
**Establish assurance processes to ensure an effective risk management program**

# RISK GOVERNANCE STRUCTURE

- **Clearly define risk oversight roles**  
(Board and sub-committees; appoint Board members/advisors with deep risk management expertise; provide risk education)
- **Align Board and management structures**  
(charters, reporting lines, approval/decision structures, information flows)
- **Risk management independence**  
(formalize reporting relationship between Chief Risk Officer and the Board/Board Risk Committee)
- **Integrate strategy and risk**  
(ensure Executive compensation risk considered)



# ROLE OF THE CRO



## **MODELLING EXPERT**

**Manage narrow risks to inform decisions**



## **STRATEGIC CONTROLLER**

**Aggregate view of risk using firm-wide risk models**

**Risk adjusted performance management system and metrics**

**Advise Executives on risk-return performance (influence capital and investments decisions)**



## **STRATEGIC ADVISOR**

**Board visibility**

**Understands strategic and operational uncertainties**

**Supports high-level risk decisions, challenges business plan assumptions and uses traditional risk controls to alter the risk profile**

**Creates process to channel risk information to key decision makers**

“

**AN EFFECTIVE CRO MUST STRIKE A BALANCE OF STRATEGIC ADVISOR,  
CONTROLLER AND MODELLING EXPERT.** (INGRID ROBINSON)

**THE ART OF SUCCESSFUL RISK MANAGEMENT IS GETTING THE  
EXECUTIVE TEAM TO SEE THE LIGHT AND VALUE THE LAMP BEARER.**  
(JOHN FRASER)

”

# RISK POLICY

## Board expectations and standards communicated:

- **Risk philosophy**
- **Governance structure**
- **Risk appetite & tolerance**
- **Risk framework and processes**  
(how parts of the organization work together)



# RISK ASSURANCE

## Board report should provide:

- **Forward-looking analysis (less historical data/trends)**
- **Key performance and risk indicators (compared to targets/limits)**
- **Actual performance of previous business/risk decisions (including rationale for management recommendations)**
- **Concise executive summary of business/risk performance (including external performance drivers)**
- **Key Board discussion/decision points**
- **Integrated view of the organization (not functional or silo views)**
- **Independent ERM assessment**

# QUESTIONS DIRECTORS SHOULD ASK

**Does the Board clearly understand its oversight mandate and role?**

**Is the Board sufficiently active in fulfilling this part of its mandate?**

**Do the directors share a common, practical understanding of their responsibility for risk oversight? Is this view the same as that of the CEO and executive team?**

**Does the Board properly distinguish its responsibility for risk oversight from risk disclosure?**

**Are the objectives of the Board's responsibility for risk understood?**

**Do Board members have an adequate, up-to-date appreciation of the nature, types and sources of risks faced by the organization?**

**Does the Board understand the interdependencies and how events or conditions occurring simultaneously can spell disaster?**

# **QUESTIONS DIRECTORS SHOULD ASK – CONT'D**

**Does the Board periodically consider and quantify the corporation's capability to take on and manage risk?**

**Are seemingly unthinkable business risks ignored because their occurrence is thought to be unlikely?**

**Does the Board have the necessary blend of business and industry knowledge and experience to assess risk?**

**Does the Board understand the differences between risk capacity, risk tolerance and risk appetite?**

**Does the Board consciously assess risk and reward when considering major strategic or tactical initiatives?**

**Does the Board have a framework within which to make meaningful judgments around risk tolerance and risk appetite?**

**Does the Board include risk management as a criterion for executive evaluation?**

**Are current compensation practices aligned or at odds with prudent risk management?**

# RISK GOVERNANCE ROADMAP: HOW, WHEN & WHERE?



#	Activity	Description	Timing*	Expected Outcome
1	<b>Establish Risk Governance Structure</b>	<b>Cascade Risk Governance Structure to:</b> <ul style="list-style-type: none"> <li>▪ CEO</li> <li>▪ CRO</li> <li>▪ SMT</li> <li>▪ Departmental management</li> </ul>	With ERM Program Implementation	<b>Defined management accountabilities for risk management that align to Board accountabilities</b>
2	<b>Review Board Terms of Reference</b>	<b>Review Board responsibilities and Risk Governance Structure (how the board as a whole works together to govern risk)</b>	<b>Annually</b>	<b>Clearly articulated Board risk oversight accountabilities</b>
3	<b>Approve Risk Policy (Risk Management &amp; Committees / Full Board)</b>	<b>Work with the CRO to develop, include:</b> <ul style="list-style-type: none"> <li>▪ Link to strategic plan</li> <li>▪ Risk philosophy</li> <li>▪ Risk governance structure</li> <li>▪ Risk appetite statements</li> <li>▪ Risk performance parameters</li> </ul>	<b>Annually</b>  * <b>TIMING WILL BE BASED ON BOARD CALENDAR</b>	<b>Articulated and communicated boundaries for acceptable risk taking, in the context of strategic objectives</b>

# RISK GOVERNANCE ROADMAP: HOW, WHEN & WHERE?



#	Activity	Description	Timing	Expected Outcome
4	<b>Oversee ERM Implementation (Risk Management Committee)</b>	Review/monitor management's ERM implementation workplan.	Over 3 - 6 months (one-time task)	Leading practice systems and infrastructure to support the Board's risk oversight objectives are in place
5	<b>Approve major risks (Risk Management Committee / Full Board)</b>	Risk Management & Audit Committee review management's register of prioritized risks ("Risk Register").  Major risks discussed with the full board vis-à-vis strategic planning session.	Annually	Board will have assurance that the strategic plan appropriately considers acceptable risk taking
6	<b>Approve risk tolerances (Full Board)</b>	Risk Management Committee work with CRO to review risk tolerances and present to the full Board for approval.	Annually	Parameters defined for allowable variation around acceptable risk, relative to strategic objectives



# RISK GOVERNANCE ROADMAP: HOW, WHEN & WHERE?



#	Activity	Description	Timing	Expected Outcome
9	<b>Review Strategic Project Risk Assessment (Risk Management Committee / Full Board)</b>	<b>Risk Management Committee will review risk assessments (submitted by management) for proposed major strategic projects, and escalate recommendations to the full Board.</b>	<b>As Needed</b>	<b>Board can ensure that major projects are pursued within established Risk Policy boundaries, while being afforded the opportunity to consider internal and external resource and stakeholder implications</b>

## **RISK GOVERNANCE ROADMAP**



### **What is the End Result?**

**By the Board setting parameters for risk and engaging management in healthy discussions regarding risk; risk informed decision making takes place, supporting establishment and pursuit of the right strategic objectives.**

# **CASE STUDY**

**CHINA AVIATION OIL**



# CASE FACTS

- **Singapore subsidiary of China Aviation Oil Holding Company**
- **November 2004 could not meet margin calls**
- **Sustained losses up to \$550 million USD**
- **CEO and Head of Finance imprisoned**



# CASE QUESTIONS

1. How did risk governance fall short?
2. What weaknesses in risk management existed?
3. How could weaknesses have been prevented?



# REMINDERS

1. **Critical Reflection due September 19<sup>th</sup>**
2. **Declare Members of Group Assignment by September 19<sup>th</sup>**
3. **Hydro One & Lehman Brothers Case due October 3<sup>rd</sup>**