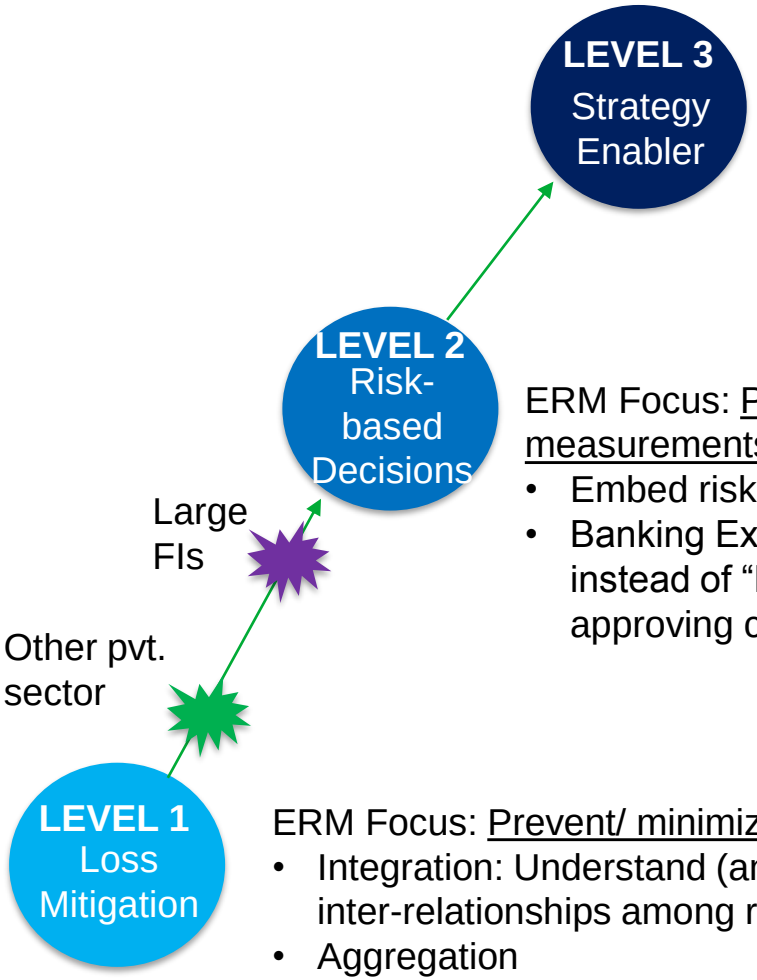
ERM:
A Private Sector View

Presentation to AFERM

Nandini Kini

January 24th, 2018

ERM In The Private Sector Is Evolving From A Loss Mitigation Function To An Enabler Of Business Strategy.



ERM Focus: ERM plays a key role in <u>identifying opportunities</u> for the front line

- Core strategy decisions and processes - such as capital allocation, market/ product selection, and organization design - are risk-based

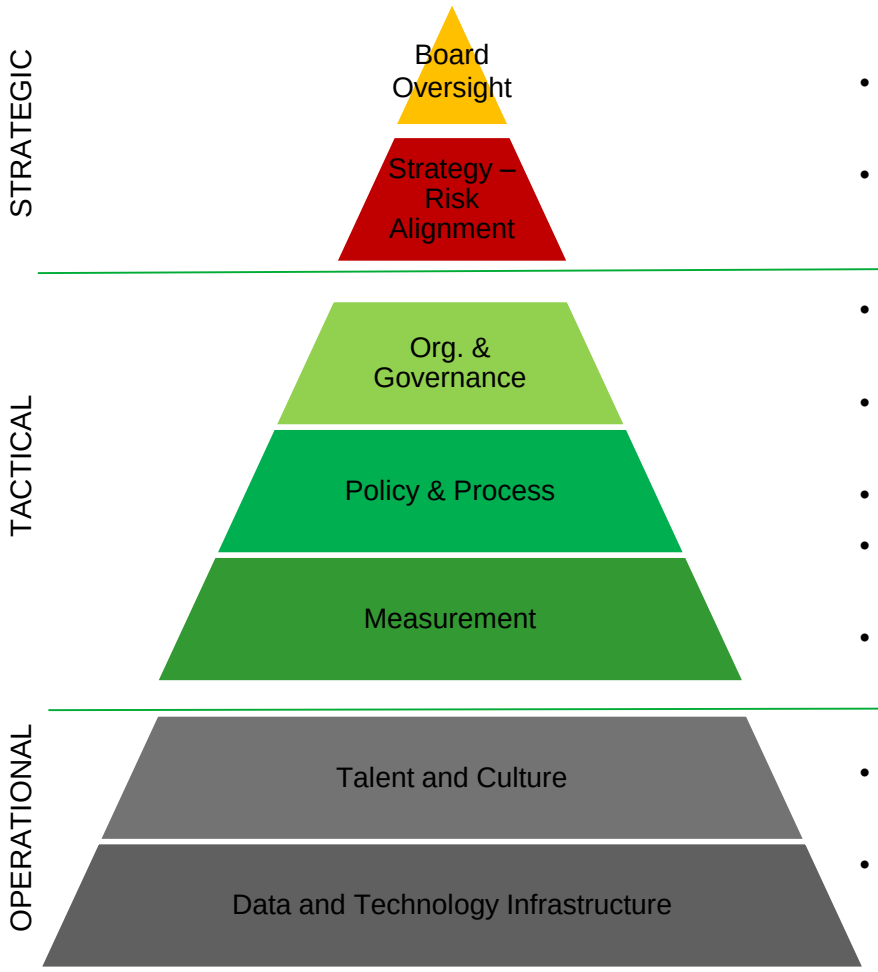
ERM Focus: <u>Providing risk assessments/ measurements as an input to front line decision making</u>

- Embed risk in performance measures
- Banking Example: “Return on Risk-Weighted Assets” instead of “Return on Capital” as a measure for approving commercial credit

ERM Focus: <u>Prevent/ minimize losses</u>

- Integration: Understand (and measure, where possible) inter-relationships among risks
- Aggregation
- For the FS industry, “check the box” for compliance

A Successful ‘Level 3’ ERM Capability Consists Of Several Layers That Are Tightly Integrated.



- The Board ensures that top risks and opportunities identified by 2nd line are evaluated while setting strategy
- Risk Appetite links strategic objectives and initiatives with measurable risk tolerances

- Front line understands and is measured on their role as the “first line of defense” for risk management
- Risk policies & processes are consistent and tightly integrated
- Integration across risk categories enables prediction
- Aggregation of risk measures enables optimal prioritization of risks and resources across the enterprise
- Culture promotes early identification of risks and issues through open communication and escalation channels

- 2nd line and key 1st line talent is trained or has experience in core risk management skills
- Enterprise-wide data governance and data quality framework; critical data elements identified and controlled

Private Sector Lessons – Do's and Don'ts

DO	DON'T
1. Demonstrating business value quickly is key to sustaining and maturing ERM – Identify quick wins and apply an iterative/ agile approach to deliver them **2. Focus on end-to-end processes, metrics, and governance first:** – Design end-to-end processes across the risk lifecycle, spanning all risk categories – For each lifecycle stage, design vertical processes to tightly link all layers **3. Develop a phased roadmap to achieve the target end state (Level 3)** – As this is a multi-year (at least 2-3 year) journey, a roadmap approach is key to realizing ROI and obtaining budget approval at regular intervals	**1. Don't focus solely on "checking the box" – i.e. reactive approach, driven by internal or external audit/ regulatory findings** – This leads to piecemeal components, but not a holistic and integrated risk framework **2. For smaller organizations, don't start with the IT/ Data build.** – Put processes, governance, and metrics in place first. **3. ERM leading practices (and related regulatory guidance) are broad and non-prescriptive by nature. Therefore:** – Don't design and implement processes/ controls without documenting the supporting rationale for all decisions – Don't assume documentation is enough. Perform regular testing/ assurance and maintain evidence of this

Emerging Leading Practices In Building Risk Culture And Talent

- **Common challenges related to risk culture and talent:**
  - Hesitation to formally identify and document control weaknesses – due to a significant increase in regulatory scrutiny, coupled with non-prescriptive regulatory guidance (e.g. on OCC Heightened Standards)
  - Individual 2nd line risk functions see ERM as "overhead"
  - 1st line view of ERM as a "documentation exercise" – resulting in low engagement in day-to-day risk identification and escalation
  - Awareness of / emphasis on risk skills in 1st line hiring/ performance evaluation is still low

- **Emerging leading practices:**
  - Risk culture/ "tone-from-the-top" employee survey (some organizations extend this to the Board)
  - Rollout of interactive/ scenario-based training for key 1st and 2nd line managers
  - Formal inclusion of "risk identification/ management meetings" in 1st line managers' calendars.
  - Additional communication channels (anonymous/ private where necessary, and usually web-based) to enable flagging of risks by staff
  - Risk skills assessment of Board and Senior Management

Case Study

A midsized regional bank [not Capital One] building ERM from first principles organized their roadmap as follows:

- **Phase 1:**
  - Metrics: Define Board-level and Risk Committee metrics across all 8 risk categories; use predictive metrics where possible
  - Data Governance/ Data Quality: In parallel, design a risk data governance & data quality framework; Implement the data quality/ data governance for a few risk data domains as a pilot

- **Phase 2:**
  - Risk Governance Structures/ Three Lines of Defense: Define/ clarify and implement the 3 LOD roles & responsibilities; Formally codify and strengthen risk governance committee charters and related processes
  - Data infrastructure: Transition risk data into the risk data warehouse in phases, to facilitate metric production
  - Data quality and controls: Define a standard risk data dictionary; Identify 'critical data elements'; Apply data quality controls to the CDEs in the data warehouse
  - Risk culture survey – enterprise-wide across 3 lines/ multiple business lines

Case Study (continued)

- **Phase 3:**
  - Build top risk identification process and analytics:
    - Integrated risk identification process involving top-down, bottom-up, and research-based activities
    - Machine learning pilots to aggregate trends from risk self-assessments/ issues data
  - Risk-based performance measures defined and implemented in the 1st line
  - Risk culture programs launched: Communications, training, and escalation channels
  - Risk talent programs enhanced, including succession planning for senior roles

- **Phase 4:**
  - Risk-based capital allocation
  - Pro-active opportunity identification for business on a monthly/ quarterly basis