Deloitte's point of view: Nine principles of Risk Intelligence

Risk Governance

- Common Definition of Risk
- Common Risk Framework
- Roles & Responsibilities
- Transparency for Governing Bodies

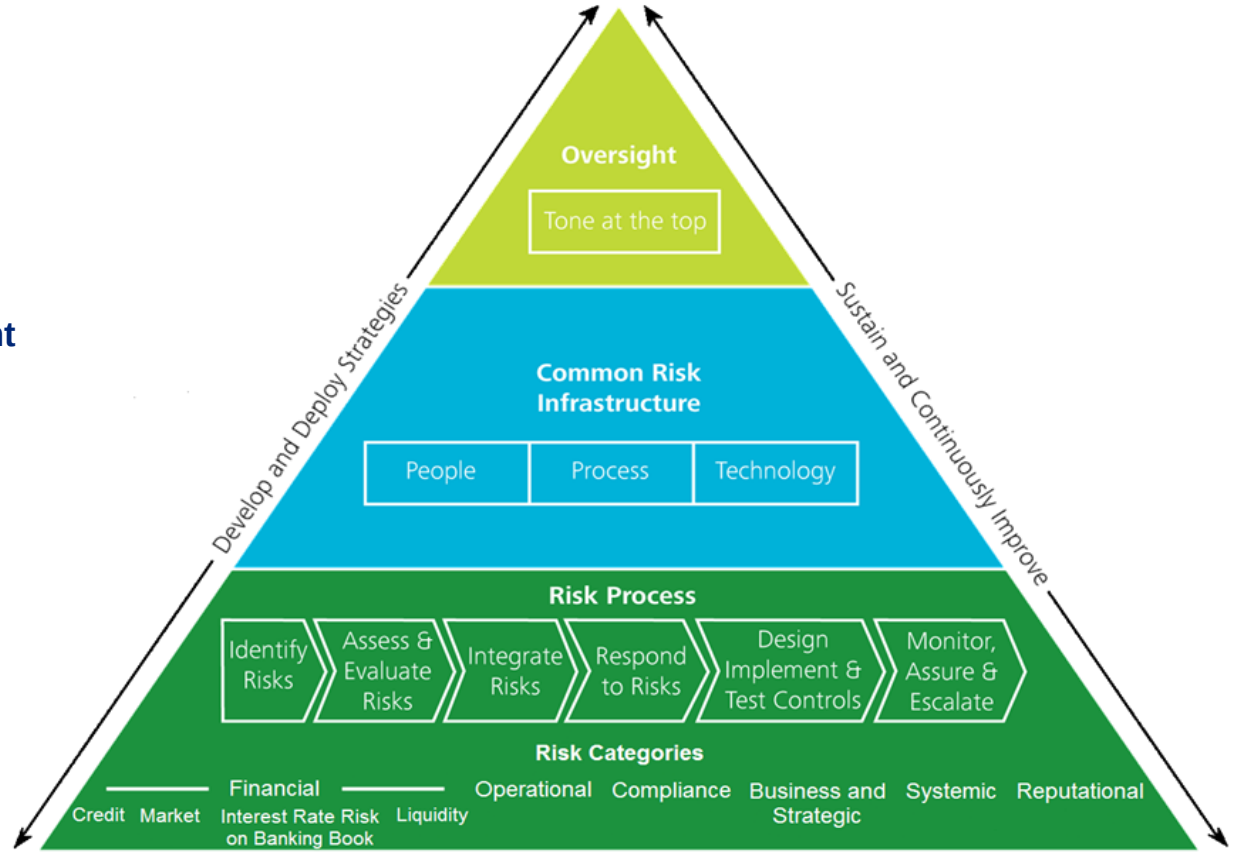
Risk Infrastructure & Oversight

- Common Risk Infrastructure
- Executive Management Responsibility
- Objective Assurance and Monitoring

Risk Ownership

- Business Unit Responsibility
- Support of Pervasive Functions

The Risk Intelligent Enterprise™



General trends, issues and notable topics

Board of Directors

- Risk program directly tied to “value-killer” or critical strategic risks
- Risk oversight is the entire board’s responsibility
- Significant raised expectations of regulators
- Reputational risk is the “meta” of all risks

Executive management

- Dashboard reporting
- Risk culture and the people side of risk management is critical and often overlooked
- Social media is a risk and opportunity
- More effort on harmonizing risk taxonomies (risk, compliance, SOX)
- Risk is a defined agenda item within executive management team meetings
- Use of technology, analytics and continuous monitoring
- IAD or outside party to perform end-to-end review/benchmarking of risk program annually

Business unit and functions

- First line of defense in a “three lines of defense” model is critical
- Senior risk leaders within each critical business units and functions
- Business units/functions must see value from program
- Business units/functions expect consistency of risk definitions, approach, tools across regulated functions (e.g., risk, internal audit, compliance, SOX)

Traditional fiduciary risk management

Key Risks — Operational, Compliance, Strategic/Business/Product, Reputation, etc.

Oversight — Board, Risk & Trust Committees; Chief/Regional Fiduciary Officers

Policies & Procedures — General, Administrative, Investments, etc.

Account reviews — Reg 9's (investment & administrative), Red Flags

Limits — Concentrations, Holdings, Discretionary Distributions, etc.

Account Lifecycle Management — Acceptance, Reviews, Distributions, Complaints, Litigation

Investments/Managers — Due Diligence, Approved Lists, Investment Policy Statements (investment objective/risk tolerance)

Specialty Areas

- Administration — Charitable/Non-Profit, ILITs, IRAs, Estate Settlement, etc.
- Assets — Closely Held Assets, Real Estate, Farm & Ranch, Oil/Gas/Minerals, etc.

Monitoring & Exception Reporting — KPIs/KRIs, ODs, UITC, Reg 9's, Investment Performance; automation of exception reporting/monitoring

Testing — Compliance, Internal Audit (little to none by Business Units)

Other Critical Areas — New Products & Initiatives, Oversight of Third Party Relationships, New Laws/Regulations

Trends in fiduciary risk management

Impact of Trends in Enterprise Risk Management on Fiduciary Risk Management

- Trends at the Enterprise level will flow down to the Fiduciary level
- Many organizations are developing “Risk Frameworks”
- FRM program will evolve to a risk-based focus, relying more on analytics and quantitative analysis
- Consistency in risk management programs firm-wide, including independent testing
- Compliance and Operational Risk Management may converge into a combined unit, or at minimum, both report to a common Enterprise Risk/Compliance function
- Establish Office of the Chief Fiduciary – differentiating fiduciary risk management from fiduciary compliance
- Establish Risk Committees in addition to traditional Trust Committee structure
  - Could be a Trust Risk Committee, or an Asset/Wealth Management Risk Committee, or Corporate-level Risk Committee
- Must be able to articulate to Line of Business and Corporate Executives the impacts of new regulation

Above will vary in degree and organizational structure based on size and complexity of the institution

- But concepts and trends will apply to all

Trends in fiduciary risk management (cont.)

Business Units Are Taking More Ownership

- Documentation of its risks and controls — risk/control matrix
  - More commonly known as “Risk-Control Self Assessment” (RCSA)
- Owning first level of (self) testing
- Owning its committee structure
  - Business executives chairing the business committees

New Ways of Looking at Fiduciary Risk — Risk Review Concept

- High level business risk review discussions with senior management and representatives from business and enterprise control functions
- Deep dive risk reviews of business units, key processes, key products/services
- Identifying needed improvements or enhancements
- Sharing results at risk committees
- Tracking progress

Interplay between Enterprise Risk Management (ERM) and Fiduciary Risk Management (FRM)

FRM is a key part of broader Enterprise Risk Management organization

- If not now at your organization, likely to be at some point in the future
- Independence from the line of business is still the key

Coordination

- FRM is no longer on its own; it's part of a broader program
- Maintain an ongoing dialog between ERM and FRM teams — particularly between fiduciary compliance teams and fiduciary risk management teams (if distinct teams)
- Ensure ERM team is involved with the FRM team and risk management process, e.g., committee participation, risk review participant, etc.
- Ensuring no gaps between banking regulations and fiduciary regulations with respect to oversight and direct responsibility; and managing overlaps

Talent and Resources

- Sharing resources, e.g., a centralized testing team
- Placing fiduciary expertise with the enterprise team
- And vice versa too

Education

- Teaching each other — business, product/service, regulatory
- Learning from your company's risk teams in other line of business as well