The Forum that Connects

COMPLIANCE & ETHICS FORUM FOR LIFE INSURERS

Conducting Risk Assessments

CEFLI Compliance Fundamentals Training Conference

Debbi Corej – Specialist Leader, Deloitte & Touche LLP

June 12, 2014

Workshop agenda

- Why is it important to conduct risk assessments?
  - Regulatory focus
  - What is ORSA?
  - Increasing expectations
- Risk management, process & basic concepts
- Integrated risk assessment model
- Examples

Summary of global regulations

Regulation	Description
Solvency II	The **Solvency II** system includes both quantitative and qualitative aspects of risk, each pillar focusing on a different regulatory component: minimum capital requirements, risk measurement and management, and disclosure. It is intended to offer insurance organizations incentives to better measure and manage their risk situation.
National Association of Insurance Commissioners (NAIC) Solvency Modernization Initiative (SMI)	The **SMI** is a critical self-examination of the United States' insurance solvency regulation framework and includes a review of international developments regarding insurance supervision, banking supervision, and international accounting standards and their potential use in U.S. insurance regulation.
NAIC Own Risk Solvency Assessment (ORSA)	The **ORSA** is a confidential internal assessment of the significant and relevant risks associated with the insurer's current business plan and the sufficiency of capital resources to support those risks. It is an important element of the Solvency II framework currently being implemented in Europe.
ComFrame	**ComFrame** will require Internationally Active Insurance Groups (IAIG) to have in place a group-wide ERM framework and be able to calculate its solvency requirements.
Federal Reserve Board (FRB) SIFI Designation	The Dodd-Frank Act authorizes the Financial Stability Oversight Council (FSOC) to require a non-bank financial company to be supervised by the FRB and subject to enhanced prudential standards if the FSOC determines the non-bank financial company as a **systemically important financial institution (SIFI)**.

Risk management and regulatory supervision are converging

- The global financial downturn crisis has sharpened the focus on enterprise risk management (ERM). Executives, prompted by boards of directors, rating agencies and regulators, are being asked to enhance processes for identifying, measuring and managing risk.
- Until recently, insurance regulatory regimes were primarily focused on formulaic capital adequacy rather than holistic risk management processes.
- Rating agencies continue to increase their focus on ERM policies, incorporating this information into their rating assessment models and requiring disclosure in data requests and ratings discussions.
- The situation has changed, and across the globe effective risk management is becoming a cornerstone of current and emerging supervisory frameworks.
- As a result, insurers are investing in ERM and implementing tools to assess capital and project earnings that reflect their risk appetite and tolerance.

cefli The Forum that Connects

Many factors are shaping risk management practices

Financial and disclosure reporting requirements

- Risk management, corporate governance and internal control related public disclosures presented to shareholders and to regulators

Supervisory requirements

- Evolving regimes requiring ORSA, capital management and risk based capital charges

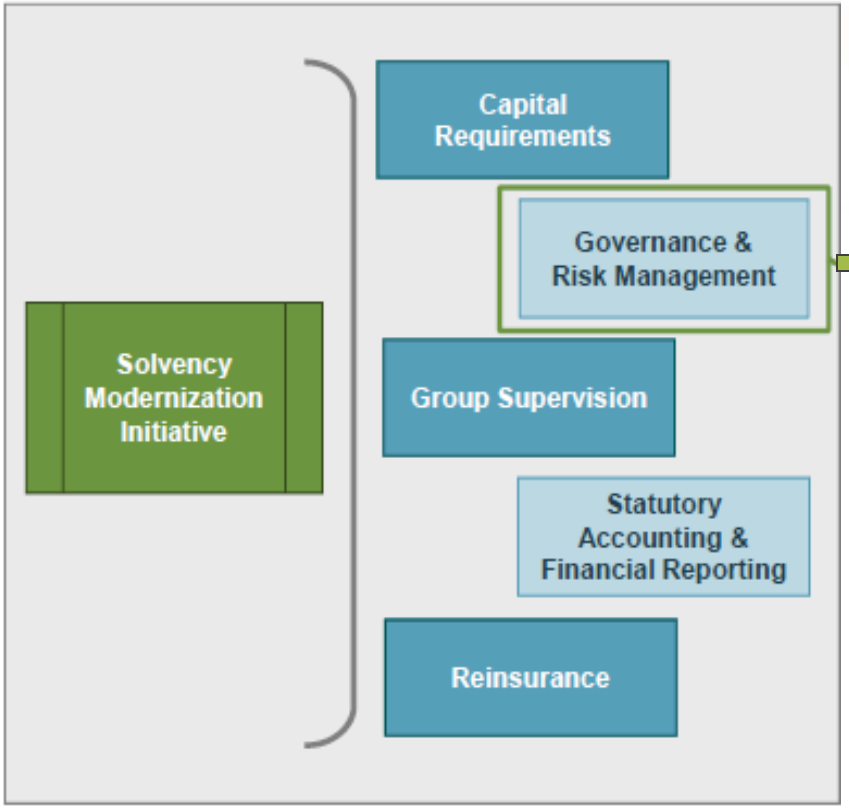
Supervisory review process

- Risk-based supervisory review process based on sound and prudent management of the business and assessment of risk management programs and system of governance

Rating agencies criteria

- ERM is one of the factors that many rating agencies take into consideration within the rating process

So what is ORSA?



Background

- The SMI was adopted by the NAIC in 2008 to respond to financial downturn and international solvency developments
- **The ORSA Model Act** adopted in September 2012 with an effective date of January 2015
- The ORSA Guidance Manual is designed to provide guidance regarding the reporting of insurer's own risk and solvency assessment
- ORSA Exemption: Individual insurer with annual gross premium < $500MM and/or Insurance groups with annual gross premium less < $1 BN

cefli
The Forum that Connects

NAIC ORSA's two key requirements

ORSA is a process

- ORSA is an insurer's own process for assessing its risk profile and the capital required to support its business plans in normal and stressed environments on a forward-looking basis
- The Guidance Manual requires insurers/insurance groups to carry out this risk and solvency assessment process on a regular basis

ORSA is a regulatory filing

- On an annual basis, insurers will be required to provide a regulatory filing that explains their ORSA process and results
- The filing does not have a prescribed format but needs to contain three sections:
  - description of ERM framework;
  - assessment of risk exposures; and
  - group risk capital and prospective solvency assessment

NAIC ORSA involves a self-assessment of the insurer's risk management framework and solvency position. Effective 1/15/2015.

cefli The Forum that Connects

ORSA Summary Report overview

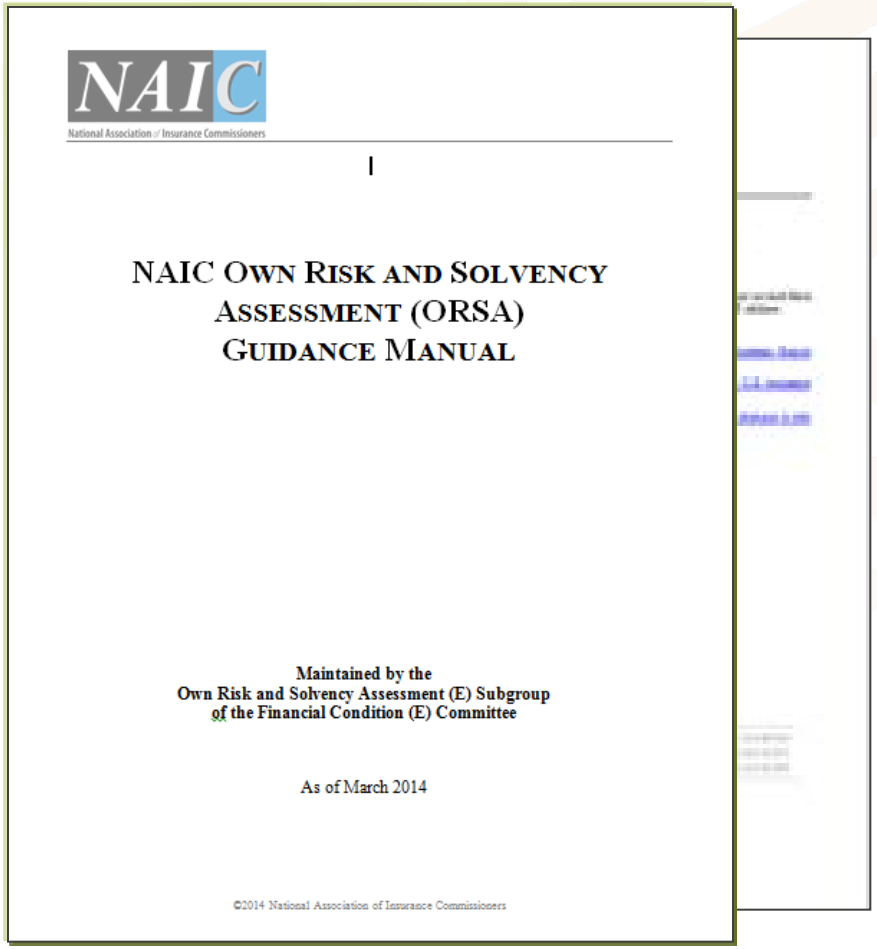
The ORSA Summary Report is currently split into three mandatory sections. The information, presentation and structure of each section are determined by the reporting entity.

Section 1: Risk Management Framework	Section 2: Assessment of Risk Exposures	**Section 3: Group Risk Capital & Prospective Solvency Assessment**
•Requires an overview of the entity's risk management framework including; • Descriptions of culture and governance • Statements on risk appetite • Tolerance limits and amount and quality of risk capital • Outlines for the process by which an entity identifies and prioritizes risks, monitors the processes and makes decisions	•Requires insurer level quantitative and qualitative assessments of risk exposures including • Relevant and material risks identified through the processes outlined in the first section and the analysis of those risks • Impact of risk scenarios capital requirements.	• This section provides a summary of the risk due to interconnectedness across groups and ability to meet future capital requirements. • The analysis should be based on the decision making process used in an entity's business plan. • Include a prospective solvency assessment at the entity level should be conducted to ensure allocated available capital meets or exceeds the required risk capital.

ORSA Guidance Manual

In March 2014, the NAIC released a revised ORSA Guidance Manual..

Link to ORSA Guidance Manual:
http://www.naic.org/committees_e_orsa_wg.htm



cefli
The Forum that Connects

Poll question

Expectations of risk management functions are increasing, where are these increasing expectations being most driven from?

- Changing regulation
- Rating agencies
- Internal business demands
- Financial analysts and shareholders
- Other/I don’t know

cefli
The Forum that Connects

Increasing expectations on the risk function

- Setting the bar higher

External factors

Regulatory

- Both domestic and international pressures

Rating agencies

- Incorporated into assessments and rating discussions

Analysts and shareholders

- Covered in results presentations
- Impacts on share price

Internal factors

Board and committees

- Seeking to understand the role of the risk function and the organization's strategic risk direction
- Placing greater attention on risk process and issues

Business

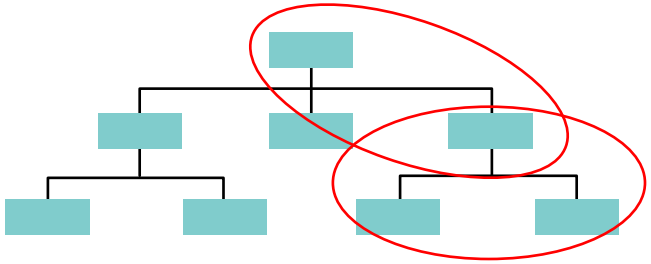
- Seeking to understand the role of the risk function
- Looking for risk insight

Other control functions

- Seeking to understand how the role of the risk function sits with current activities and responsibilities

Enterprise-wide Risk Management ("ERM")

Company Structure

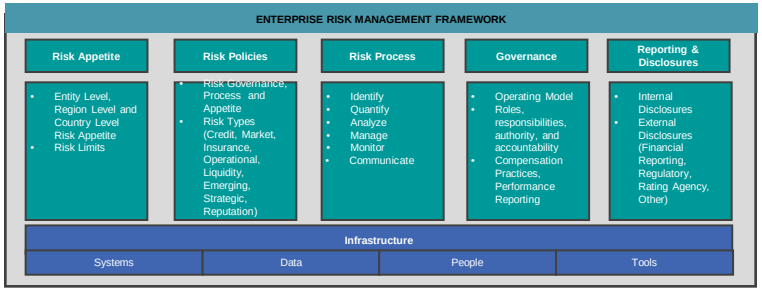


Group

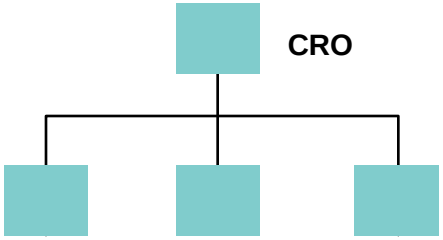
Regions / BU

BU /Affiliates

ERM Framework



Risk Operating Model



Companies organize themselves in many different ways to address market opportunities, geographic location, customer services, etc..

An ERM Framework must cover all of the risks within the business to be considered enterprise wide.

A Risk Operating Model or target operating model needs to do two things:

1. Overlay the company structure completely
2. Deliver the enterprise wide risk management framework across all risks

cefli The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Proposed ERM principles and objectives

Guiding Principles

Oversight of ERM is provided by the board, and risk committees. An executive risk committee chaired by the CRO with a reporting line to the CEO provides unrestricted access to the board for the oversight of key risks

ERM responsibilities are focused on policy setting, limit setting, risk monitoring and oversight activities and excludes front line management of risk (i.e., execution of hedging strategy, derivative overlap/balance sheet overlay, reinsurance, etc.)

The risk management function supports compliance with industry and rating agency expectations as well as regional/global regulatory requirements as required

Objectives

The objective of ERM is the establishment of an ongoing, positive risk management culture within the organization that:

- Embeds risk and risk management considerations in strategic and everyday decision-making
- Creates awareness of risks and risk appetite at all levels in the Company's business lines
- Manages risks in a holistic and transparent manner within the Company's predetermined risk appetite, weighing both downside risks, policyholder protection and upside opportunities
- Creates an effective and efficient governance structure with well defined roles, responsibilities, authorities and accountabilities
- Creates a clearly articulated approach to identifying, quantifying, evaluating, and monitoring risk/return trade-offs
- Communicates the risk appetite and management of risks clearly to both internal and external audiences

ERM Framework

- High level summary of key ERM elements
- Identification and assessment of relevant and material risks for executed business strategy
- Documentation of assessment tools
- Description of accounting basis and legal entity structure
- Definition of critical risk management policies and procedures

cefli
The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Risk culture and risk appetite

Risk culture is about the entire organization, not just the Risk function. At the highest level, risk appetite defines the amount of overall risk that a firm is willing to accept in pursuit of its business objectives.

- Risk Culture encompasses the general awareness, attitudes, and behaviors of an organization's employees toward risk and how risk is managed within the organization.
- Risk Culture is a key indicator of how widely an organization's risk management policies and practices have been adopted
- Risk appetite principles
  - Defined by senior management and approved by the board of directors
  - Aligned with business objectives and should be linked to key risk indicators (KRIs)
  - Responsibility distributed across the organization to all levels of management
  - Embedded in policy development, business and strategic planning, resource allocation, and various business and risk processes

cefli The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Understanding risk culture

Culture is influenced by an organization's symbols, management systems and behavioral norms. When seeking to understand an organization's risk culture, four main organizational influencers of risk culture (risk competence, motivation, relationships and organizational risk environment) can be assessed by analyzing 16 key indicators of risk culture.

Organizational culture

Organizational symbols Inherent interpretations of symbolic messages	■ How time is spent ■ Where resources are invested ■ The physical environment/layout ■ What is rewarded ■ Who is rewarded ■ Value statements
Management systems Organizational processes and infrastructure	■ Strategy development process ■ Goal setting/budgeting process ■ Organization design ■ Business process design ■ Reporting and measurement ■ Performance management ■ Incentives and rewards ■ Communication methods
Behavioral norms Accepted patterns of behavior visible across an Organization	■ How leaders, managers and key influencers act with employees ■ What employees expect to be said or done ■ How people work: one-on-one, in teams, or in larger forums ■ How employees interact with peers, managers and internal customers

Risk culture framework

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Three lines of defense

Risk management responsibility can be viewed as three lines of defense: Management, Chief Risk Officer (CRO)/Risk function, and Internal Audit.

Board of Directors

First line of defense	Second line of defense	Third line of defense
Top management and new business dev.	**Risk management function**	**Internal audit**
■ Promote a strong risk culture and sustainable risk-return decision making ■ Portfolio optimization on the macro and micro level ■ Promote a strong culture of adhering to limits and managing risk exposure ■ Ongoing monitoring of risks	■ Combination of watchdog, trusted advisor, enforcer ■ Understand how the business makes money—and actively challenge initiatives if appropriate ■ Top talent with business experience engaging with management and NBD as equals ■ Independent from management and staff that originate risk exposures ■ Overarching risk oversight unit across all risk types and business units	■ Good understanding of the business and risk management ■ Top talent within audit—to challenge the front office and risk management function ■ Independent oversight function with ability to enforce fulfillment of findings ■ Ability to link business and risk with process and IT know-how

External auditor

Regulator

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Risk process

There are five key processes within a robust risk management framework:

1 Risk identification

- Structured around enterprise wide framework of risk categories and definitions
- Both top down and bottom up process
- External event monitoring
- Scenario Analysis
- Emerging Risks

2 Risk assessment

- Need BU involvement
- Provide a qualitative and quantitative view of risk
- Assessed on the Gross/Inherent basis and on the Net/Residual basis taking into consideration existence of risk mitigation
- Level of complexity of the risk assessment should correlate to level of significance of the risk

3 Risk measurement

- Range of risk measurement methodologies exist
- Data availability and quality is key
- Most start with qualitative form of risk assessment
- Examples include: risk assessment and scoring, KRIs, loss event and scenario modeling, economic capital modeling and allocation

4 Risk response and mitigation

- Appropriate response is dependent on company's strategic objectives, risk appetite, level of action required and return/reward/cost of the mitigation plan
- Can range from fully mitigate to partial mitigation, to accept and no mitigation
- Establish a risk mitigation framework

5 Risk monitoring and reporting

- Risks usually monitored individually and then aggregated and reported
- RM Function usually aggregates and reports
- Effective risk reporting should include info on key risks enterprise wide, provide clear picture of risk profile, emerging risks, focus on KRIs, limits and thresholds
- Risk dashboard

Risk assessments

Types of Risk	Assessment Considerations for all Types of Risk
Market Risk	Relevant and material risks - Broad and holistic view
Credit Risk	Both quantitative and qualitative
Insurance	Forward looking under normal and stressed environments
Operational	Model validation, calibration and assumption setting process
Compliance	Multiple perspectives including regulatory, economic, business, etc.
Other – Business Specific	Tolerances and limits setting process. Priority ranking/rating of material risks.

Risk measures

A range of risk measurement methodologies exist from initial to advanced. Organizations will have to mature their ~~its~~ risk measurement capabilities in accordance with their ~~its~~ overall ERM measurement framework.

Risk Assessment and Scoring

Key Characteristics

- Risk framework
- Self-assessment
- Assessable entities are identified
- Impact and Likelihood
- Unmitigated Risk, Control Effectiveness, and Residual Risk
- Quantitative Risk Scale
- High, Medium, Low dollar thresholds
- Risk Scoring, Analysis and Quantification

Key Risk Indicators (KRIs)

Key Characteristics

- Indicators relevant as proxy's of risk levels for different risk types
- Possible metrics categories include those indicative of business volume, operational efficiency, error rates, losses or potential losses, control effectiveness
- Indicators selected should be relevant as risk measures for specific risks and analyzed whether they are leading, lagging or coincident risk measures

Loss Event and Scenario Modeling

Key Characteristics

- External and Internal Loss event categories identified
- Loss event database
- Causation factors captured
- Near misses captured
- Direct and Indirect Costs are tracked
- Thresholds set for reporting
- Scenario modeling performed by business experts to supplement loss data

Economic Capital Modeling and Allocation

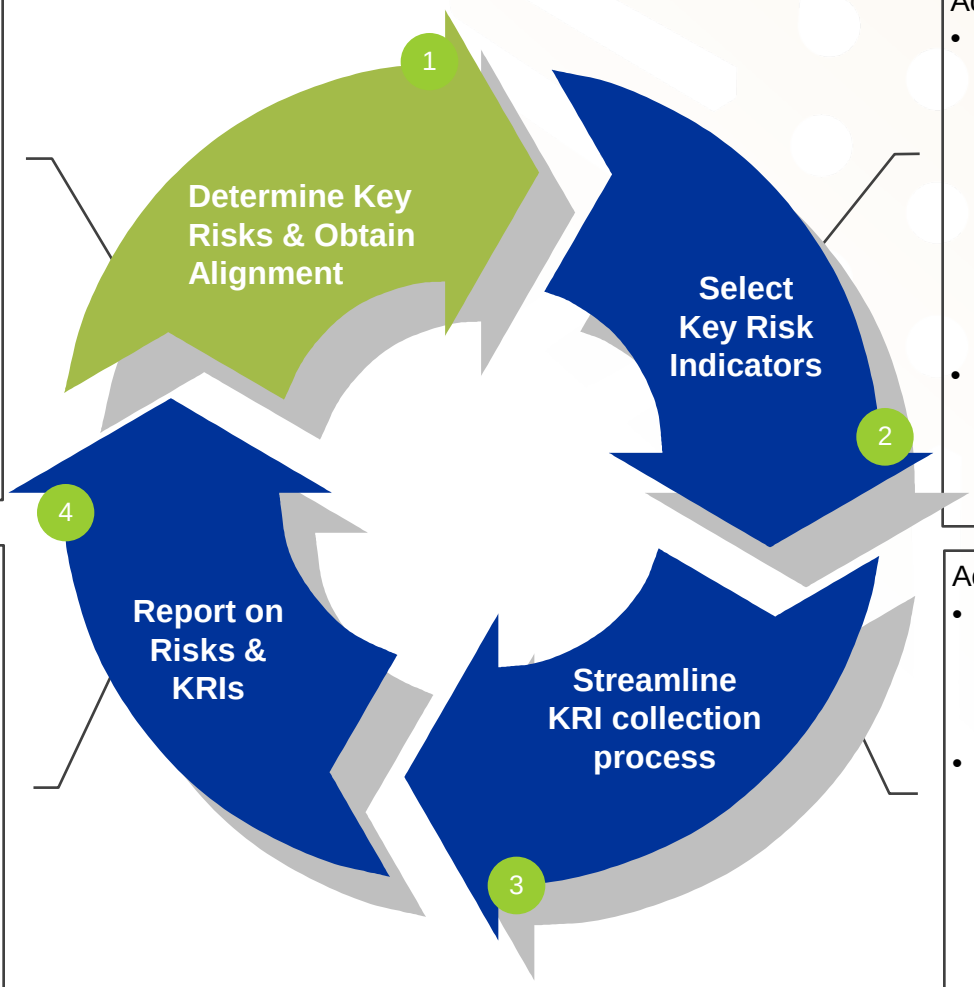
Key Characteristics

- Overall framework and methodology for determining and allocating economic capital (EC)
- Methodologies should address all relevant risk types for entity
- Loss distribution (frequency and severity)
- Statistical models to estimate risk exposure
- Calculation engines (e.g., Monte Carlo simulation engine for Value at Risk)

Key Risk Indicators (KRIs)

Follow a structured approach to fill in the gaps and refine the list of key risks, KRIs and Metrics.

Activities:
- Determine reporting requirements and obtain alignment with executive management and key stakeholders on identified key operational risks



Activities:
- Meetings with process owners to prioritize key risk indicators based on factors such as:
  - Effectiveness to measure Key Risk
  - Availability of existing KRIs
  - Feasibility of collection
- Determine KRI parameters such as:
  - KRI weights
  - Risk Thresholds

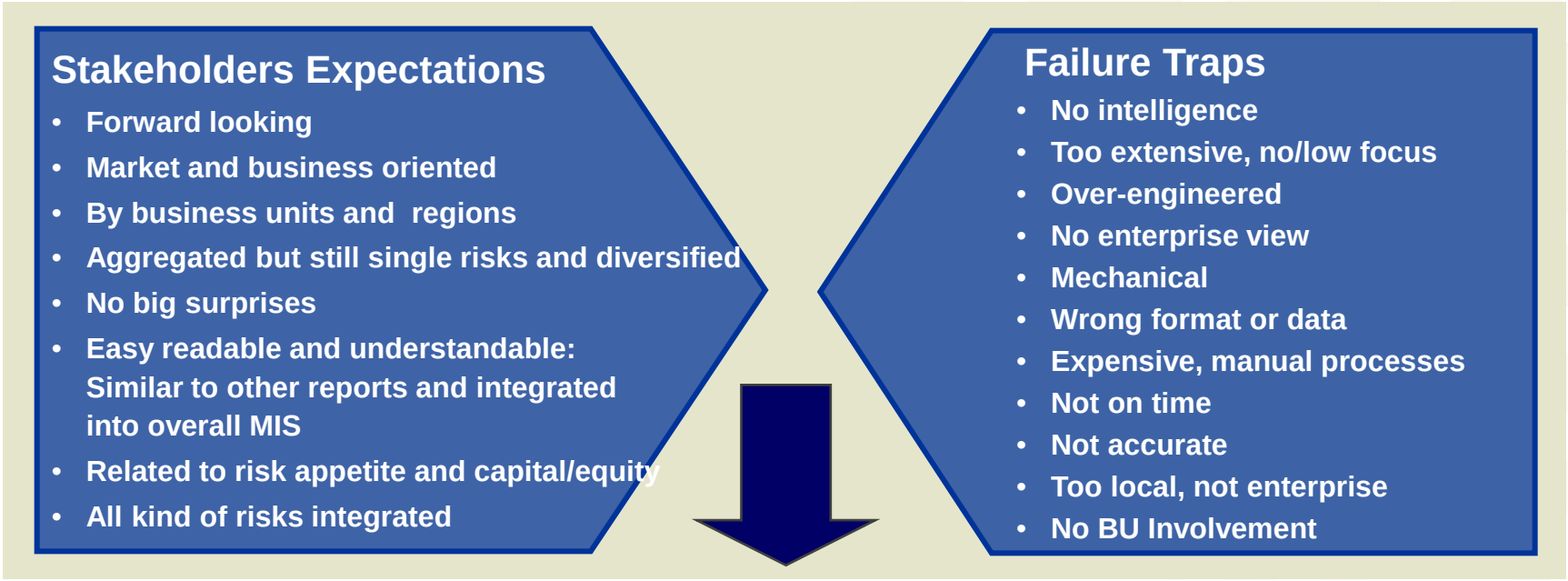
Activities:
- Analyze KRI data and determine trends based on KRI parameters
- Determine Composite Risk Indicators to get an understanding of risk levels
- Periodically evaluate effectiveness of KRIs

Activities:
- Identify KRI owner(s) and determine how metrics are currently collected and reported
- Identify opportunities to automate the data collection process

cefli The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Risk reporting



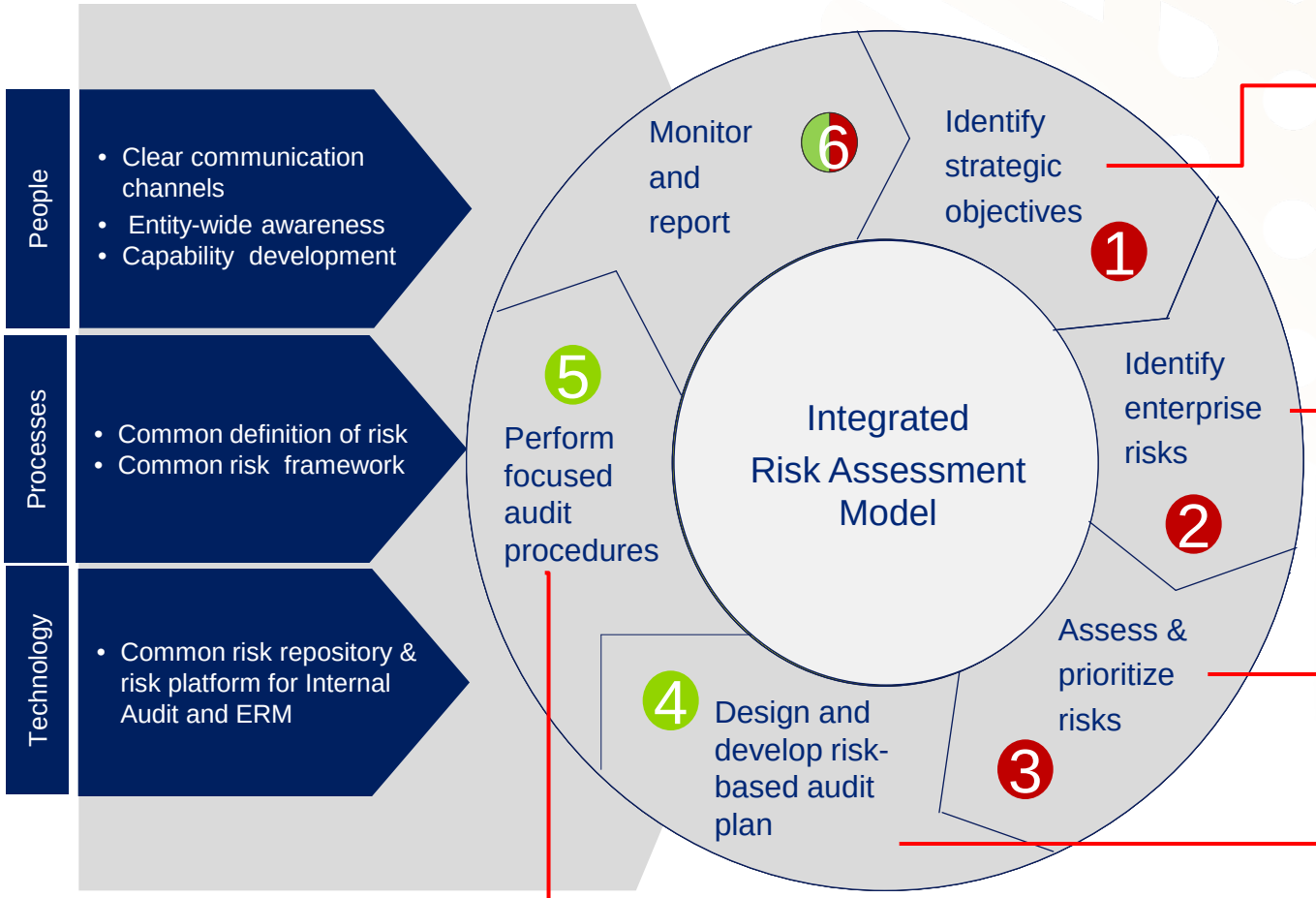
Basic Principles of Risk Reporting

- Clear and consistent risk language
- Simplicity to Reporting structure
- Transparent and understandable
- Objective and reliable
- Precise
- Complete
- Adequate
- Unbiased

cefli The Forum that Connects

Integrated Risk Assessment Model - Illustrative

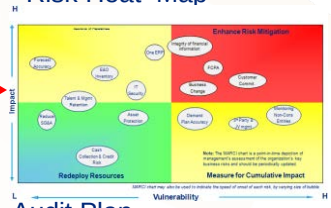
Below is a sample approach and tools for conducting an integrated risk assessment:



Shareholder Value Map

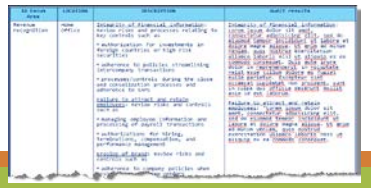
Risk Intelligence Map

Risk Heat Map



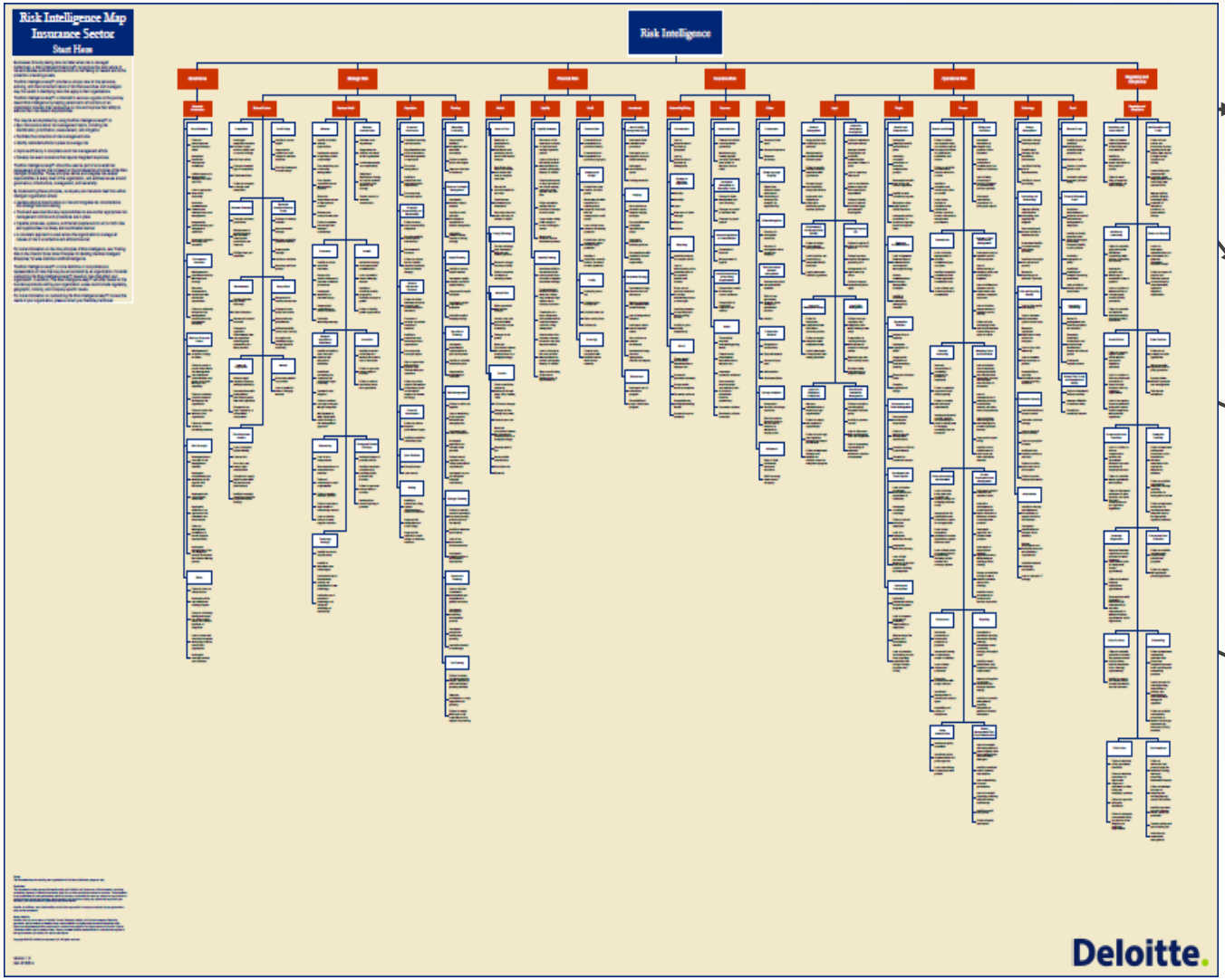
Audit Plan

Audit Procedures & Results



Copyright © 2014 Deloitte Development LLC. All rights reserved.

Common Risk Taxonomy - Example



- Level 1: Risk Classes
- Level 2: Risk Categories
- Level 3: Risk Sub-Categories
- Level 4: Individual Risks

cefli
The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Common Risk Taxonomy - Example (cont'd)

Level 1: Risk Classes

Risk Classes represent the highest level of risk groupings, broken down by major business activities

Level 2: Risk Categories

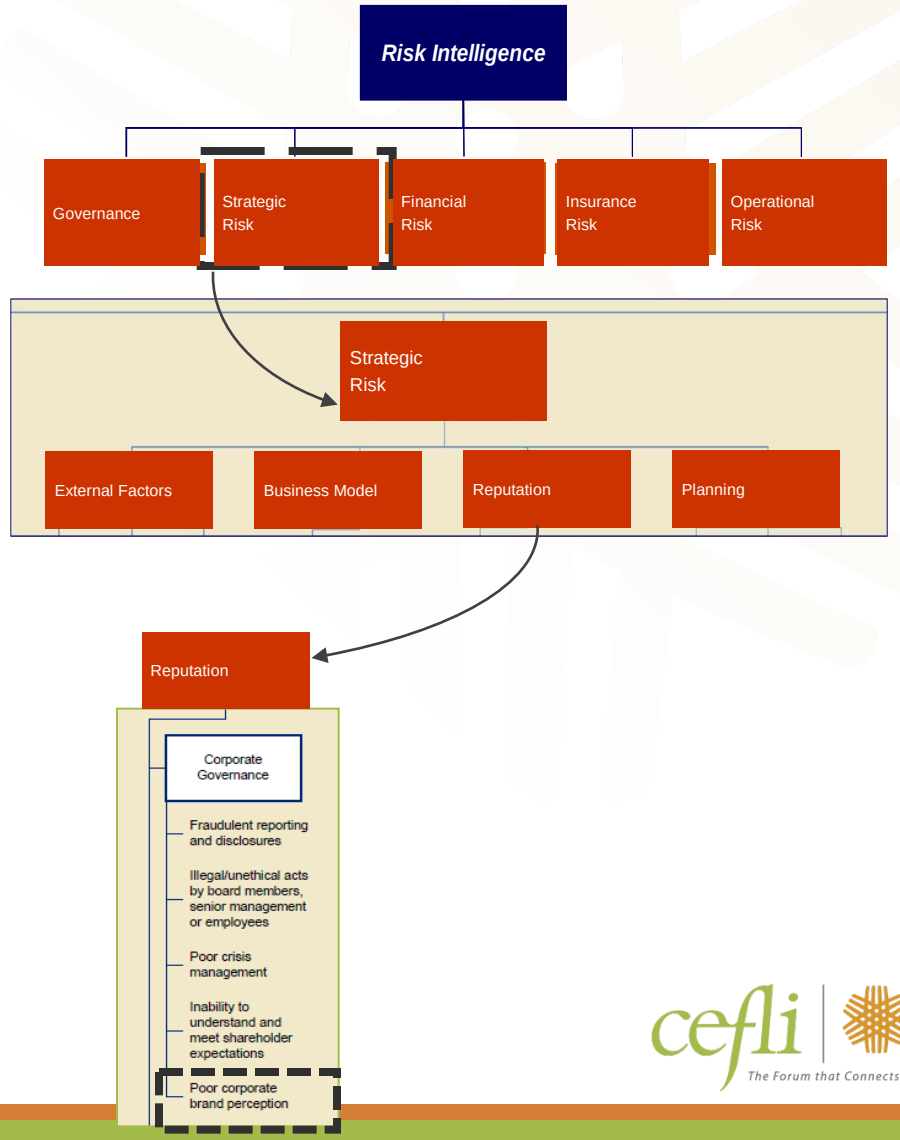
Risk Categories further classify the Risk Classes in an organization

Level 3: Risk Sub-Categories

Categories are further broken down to Sub-Categories in order to structure the individual risks

Level 4: Individual Risks

Individual Risks are examples of events that could negatively impact the achievement of an organization's objectives.



cefli The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Risk assessment – Example

The Risk Impact Table combines financial and non-financial description:

Tier 2 Risk Event	Key mitigation strategies in place	Known control weaknesses	Impact		Likelihood (1/20)	KRI's
			Financial	Member/ reputation		
1. Accidental acts or events causing death or injury to employees	1. Workplace/office safety measures 2. Workplace/office security measures 3. Travel risk management (TRM) program (covers business travelers and employees assigned overseas) 4. Employee event security 5. Succession planning for key employees	None	$7 million (See note 1 on calculations slide)	2	5%	▪ Number of accidents adversely impacting the business ▪ Number of willful damage incidents impacting the business
2. Accidental acts or events causing death or injury to CEO or senior officers	1. Workplace/office safety measures 2. Workplace/office security measures 3. Residential security measures 4. Business and personal travel security measures, to include TRM program 5. Event security and transportation measures 6. Security/threat intelligence sources and support services 7. Succession planning for key employees	None	$0 (See note 2 on calculations slide)	3	5%	

cefli The Forum that Connects

Risk assessments - help the business prioritize metrics and goals – an example

	Pricing and product development	In-force management	Risk mitigation	Performance metrics
Basis focus	• Statutory • Lifetime Internal Rate of Return • Single year of issue	• Chief Financial Officer's primary driver of earnings • Generally accepted accounting principles (GAAP) • Annual basis, aggregate	• Economic • Risk-neutral pricing of derivatives	• Economic capital (EC)
Issue	• Doesn't project GAAP or EC-based impacts over time	• Disconnected from product approval process	• Mitigates risk on a basis different than that on which it's priced • Complex to project impact of mitigation on accounting	• Rewards performance on a basis different than that on which product strategy is based
ERM value-add	← The risk function can facilitate the agreement of metrics that are used from pricing to performance →			

cefli The Forum that Connects

Risk assessment considerations - Effectively managing risk to reputation

Proactive management of risk to reputation

Anticipation	Of threats to strategy and opportunities for enhancement
Analysis	Of trends which may lead either to threats or opportunities
Action	On reputational levers and corporate behaviors to assure successful strategic execution

An example implemented through three reporting mechanisms:

- An alert service of emerging risks, picked up by software and vetted by humans, for operational management
- Online reporting or risks to reputation and opportunities for strategic enhancement for senior management
- Quarterly presentations to top management of major trends requiring change to corporate behavior that could impact strategic outcomes

Risk assessments can help achieve risk intelligence

Risk Intelligence is a philosophy that is focused on maintaining the right balance between risk and reward. Simply put, organizations create value by taking risks and lose value by failing to manage them. An effective risk management program focuses simultaneously on value protection and value creation.

Mature Level of Risk Intelligence
• Appropriate business units are actively engaged in ERM
• Potential threats and opportunities are identified
• Tools and techniques are applied prospectively
• Data is captured to manage risk to within tolerances
• An early warning system is in place

cefli The Forum that Connects

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Questions.

cefli
The Forum that Connects

© CEFLI 2013. All Rights Reserved.

THE FORUM THAT CONNECTS.

cefli

Compliance & Ethics Forum for Life Insurers
P.O. Box 30940
Bethesda, MD 20824

www.cefli.org

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.