Risk Framework Assessment

Maturity Model – Case Study Illustration

Loyola University, Chicago

Varun Agarwal, PhD, CFA
Enterprise Risk Management

October 2, 2023

Topics of Discussion

1

Risk Assessment

This section presents the purpose, benefits and methodology for performing a risk assessment for an auto and home insurer

Purpose and Benefits of Risk Assessment

Purpose

- Conduct an assessment aiming at establishing a **current state** of risk capabilities
- Define a high level **target state** for this function
- Determine gaps and recommendations
- Devise path for **pragmatic** state (is it **optimized** or **best**?)

Key benefits to the Insurer

- Assessment results aligned to increase the efficiency and efficacy of risk function
- Improved delineation of the areas of accountability for the 3LoD areas
- Establish a reference point for improving the risk function
- Identify potential synergies between company's principal functions
- Provide contextualization between insurer and external industry peers
- Risk function improvement opportunities identified and prioritized
- Recommendations for improvement to obtain optimized value

Assessment Sources

- Assessment was based on house industry leaders' opinion, expert judgment, benchmark
- Internal stakeholder responses are a simple mean of ratings provided in interviews
- Assessor's Subject Matter Expertise
- Industry benchmarking

Challenges

- Willingness – Risk Culture
- Ability
- Priority in the organization
- Shifting industry paradigm changes (digital competition, AI, non-regulated insurers)
    - Is your risk strategy able to keep pace?
- Regulation
    - Existing
    - New
    - Challenge of meeting different (and sometimes contradictory) regimes

Assessment Methodology

- Identify framework
- Standardize definitions
- Confirm stakeholders and project expectations
- Request documentation
- Schedule stakeholder interviews
- Design benchmarking approach

- Request documents
- Conduct stakeholder interviews
- Document gaps and enhancement areas
- Communication - meet periodically w/ executives and sponsors for status updates

- Send benchmarking survey to insurer's peers
- Tap existing industry forums
- Review external study results
- Incorporate in final analysis

- Present path to maturity

The level of maturity is assessed across 6 capability areas and on a scale of 1- 4 (4 being the highest level of confidence)

.

Risk Maturity Model (page 1 of 2) (*Example*)

Microsoft Excel Worksheet

	Foundational	Compliance	Optimized	Integrated
	(Level 1)	(Level 2)	(Level 3)	(Level 4)
Business Model & Risk Strategic Alignment	• Risk Appetite not formalized • Lines of Business (LoBs), Risk, Finance & Strategy not aligned • Business activities not assessed for risk • Risk culture ineffective	• Risk Appetite reviewed only for regulatory purposes • LoBs, Risk, Finance & Strategy infrequently aligned • Business activities partially assessed for risk • Risk culture a concern	• Risk appetite reviewed less than once a year • LoBs, Risk, Finance & Strategy aligned for budgeting • Business activities assessed reactively for risk • Risk culture value realized but not ingrained	• Risk appetite reviewed at least annually • LoBs, Risk, Finance & Strategy aligned • Business activities assessed proactively for risk • Risk culture ingrained
Risk Governance & Operating Models	• 3 LoD structure absent • Risk committees do not cover key risks • ORM practices inconsistent	• 3 LoDs in defining stage • Risk committees partially cover key risks • ORM practices partially inconsistent	• 3 LoDs partially implemented • Risk committees comprehensively cover risks • ORM practices consistent	• 3 LoDs fully functional • Risk committees cover risks in an integrated manner • ORM practices consistent & integrated
Functions, Process & Effective Controls	• Risk does not allocate its cost to LoBs • Does not follow risk management lifecycle • Does not focus on improving business performance • Risk program not cost effective • Process for communicating, monitoring, and reporting risks baseline • Regulatory and MI reporting not tied together • LoB leaders do not participate in identifying risks	• Risk allocates its cost only to key LoBs • Risk management lifecycle components addressed in silos • Partial focus on improving business performance • Cost effectiveness of risk program in progress • Process for communicating, monitoring, and reporting risks advancing • Regulatory and MI reporting partially tied together • Only key LoB leaders participate in identifying risks	• Risk allocates its cost to all LoBs • Risk management lifecycle not integrated • Focus on improving business performance included in cost accounting • Cost effectiveness of risk program efficient • Process for communicating, monitoring, and reporting risks optimized • Regulatory and MI reporting tied but not well integrated • All LoB leaders participate in identifying risks	• Risk allocates its cost to all LoBs and corporate functions • Risk management lifecycle well-functioning • Focus on improving business performance integrated • Risk program cost effective • Process for communicating, monitoring, and reporting risks integrated • Regulatory and MI reporting fully tied together • All LoB leaders and corporate functions participate in identifying risks

Question: What is the best stage?

Risk Maturity Model (page 2 of 2) (*Example*)

	Foundational	Compliance	Optimized	Integrated
	(Level 1)	(Level 2)	(Level 3)	(Level 4)
Data & Risk Information Management	• Risk data not identified and risk not quantified • No aggregation of risk metrics for reporting	• Risk data identification and risk quantification in progress • Aggregation of risk metrics for reporting partial	• Risk data identified and risk quantified for regulatory purposes only • Aggregation of risk metrics for reporting not fully integrated	• All risk data identified and risk quantified • Aggregation of risk metrics for reporting completed
Risk Analytics & Measurements	• Model risk management not included in risk • Risk not quantified • Report on risks only • No stress or reverse stress testing program	• Inclusion of model risk management in risk inefficient • Risk quantified for reserves only • Report on risks and the controls needed to mitigate those risks • Only stress testing program in place	• Inclusion of model risk management in risk partially efficient • Risk quantified for reserves and pricing • Controls implemented to mitigate identified risks • Has both stress testing and reverse stress testing programs	• Inclusion of model risk management in risk sustainable process • risk quantified for reserves, pricing and capital allocation • Risk reporting drives timely action • Has stress testing, reverse stress testing and recovery & resolution programs
Risk Technology & Infrastructure	• No Third Party Risk Management (TPRM) • No GRC solution • Cyber risks not part of formal US risk program	• TPRM in progress • GRC solution partially deployed • Cyber risk inclusion in US risk program in progress	• TPRM efficient • GRC solution efficient • Cyber risk inclusion in US risk program comprehensive	• TPRM integrated • GRC solution integrated • Cyber risk inclusion in US risk program integrated

Question: What is the best stage?

Summary: Stakeholder assessment current state (*Illustration*)

Current state as assessed by internal stakeholders

	Foundational (Level 1)	Compliance (Level 2)	Optimized (Level 3)	Integrated (Level 4)
Business Model & Risk Strategic Alignment				
Risk Governance & Operating Models				
Functions, Processes & Effective Controls				
Data & Risk Information Management				
Risk Analytics & Measurements				
Risk Technology & Infrastructure				
Overall	**Foundational**	**Compliance**	**Optimized**	**Integrated**

2 Risk Assessment Results

- **Gap Assessment**

This section presents illustration of risk analyses

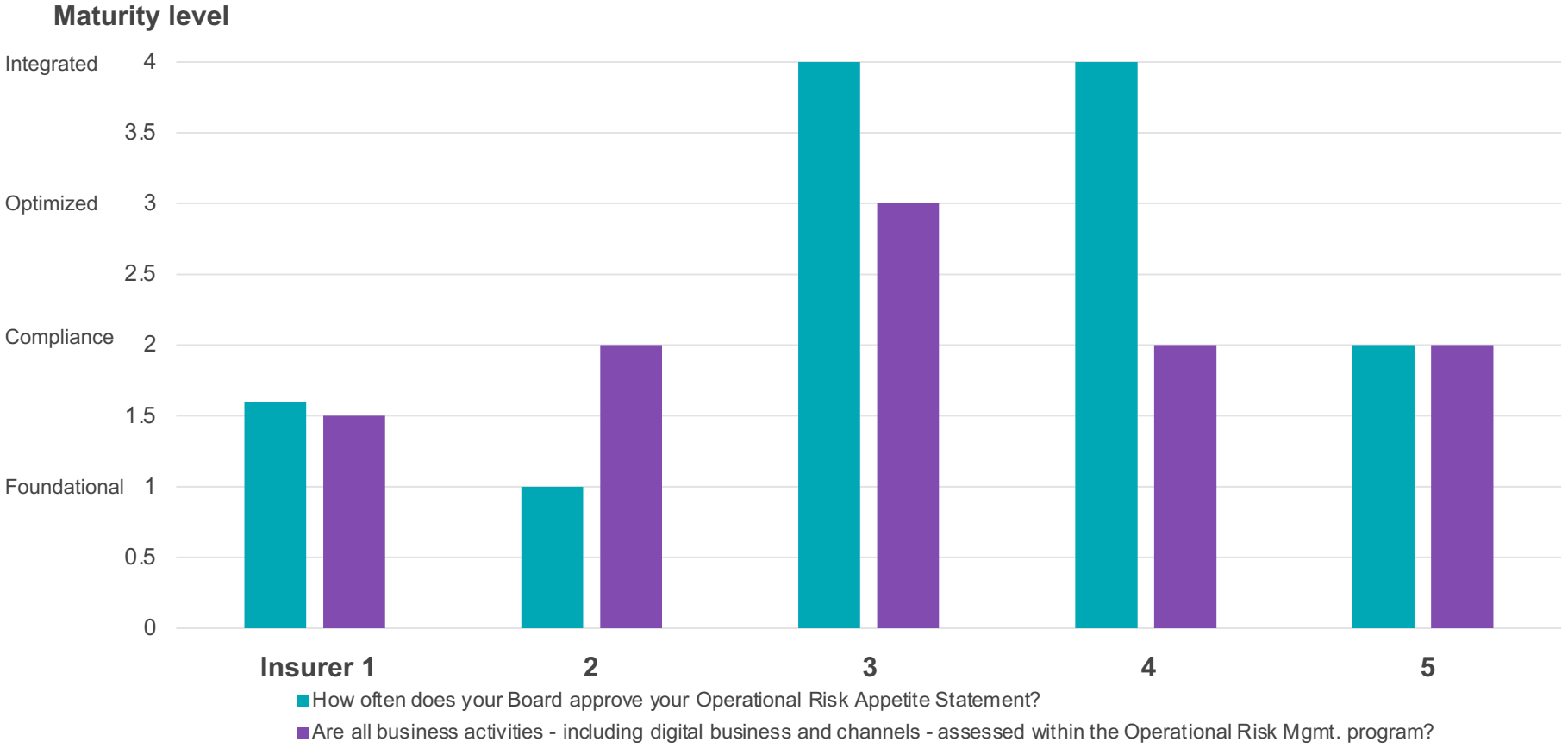
Business model & risk strategic alignment (*Illustration*)

Capabilities attributes	Current state gaps	Leading practices
1. Alignment of Business, Finance, Risk and Strategy 2. Risk appetite statement 3. Risk assessment of activities performed by business. 4. Risk culture & its awareness	• 1A – A formal risk strategy that lists the purpose/objectives, stakeholders, participants, interaction and linkage of Risk Function with outside units such as Finance, Businesses, Corporate Strategy is not well documented and not widely circulated. • 1B – While there is awareness of importance of link between business strategy and risk, it is not implemented effectively. • 1C – Bottom--up and top-down risk processes do not seem to gel seamlessly. While risk management participation from top-down perspective is well-executed, and the bottom-up process is based on the RCSA activities, there is no common frame of reference to link the two processes. Self-assessment needs to be enhanced. • 1D – Risk Function does not comprehensively participate in managing key qualitative risks in business; it also does not have active participation in Global Risk's Stress Testing program for these risks. • 1E – While Risk Function performs knowledge transfer to various groups in the organization, there is no formal Risk Training program. • 1F – There is need to execute, enhance and accelerate risk management processes more widely in the organization. • 1G – Risk Appetite is not informative.	• Superior communication, one risk taxonomy, single source of truth for data, common metadata. Risk strategy assists in managing risks proactively and comprehensively. • Risk is perceived as a partner (opposed from being restricting) to business; raise status of Risk function in the company. • **A well-developed risk appetite statement is the risk philosophy** of the organization that drives risk and corporate strategy. It also makes the organization more efficient in being able to execute its risk strategy. • Developing a robust risk culture results in little ambiguity in understanding risk objectives. • What is the **Tone from the Top?** • A strong risk culture inculcates uniform values, beliefs, knowledge, attitude and understanding of risk; encourages clear, open and upward risk thinking and risk communication, sharing of knowledge and leading industry practices, continuous process improvement, and eventually effective risk management across the organization.

Only key capability attributes are listed here (all capabilities are fully captured in the benchmarking survey that is attached in the later part of this document).

Items in dark blue font are key gaps and closing them will yield quick benefits and accelerate the establishment of a foundation to achieve an "Optimized" future state

Peer comparison: Business Model & Risk Strategic alignment



3 Risk Assessment Results
• Recommendations

This section presents recommendations that are organized into major themes for improvement of the Risk Function Risk.

Executive Summary (*Illustration*)

Risk Management is guided by conceptually sound frameworks - it should now focus intently on increasing the effectiveness of its execution

Risk Management clearly on a path towards "Optimized" level of maturity

The Risk Operations function is currently at the "Compliance" level of maturity with key activities underway that are driving momentum towards an overall "Optimized" level. While Insurer's current risk frameworks exhibit good conceptual soundness, the industry is far from full adoption of best practices. Thus, a key priority of this function should be increasing execution effectiveness by implementing a few recommendations that will derive quick benefits and accelerate the establishment of a foundation to achieve an "Optimized" future state.

Three High Priority and High Impact Recommendation Themes*

1. **Empower risk governance by formalizing three lines of defense**
   A disciplined implementation of the 3 Lines of Defense (3 LoD) model.

2. **Increase organization's coverage of self-assessment next year – regulators also want this**
   Risk leadership of RCSA program will activate and catalyze critical risk identification, data management, risk measurement, and risk IT implementation and reporting activity whilst promoting risk education and engender a positive risk culture.

3. **Risk Operations - Lead the way for Insurer in terms of risk data and informatics**
   The lifeblood of proactive risk management at the executive and board levels will require a commitment to establishing ownership and access to key risk data as well as establishing a data risk governance structure that will support effective risk reporting.

Formalize, create & "socialize" risk strategy (*Illustration*)

Theme: Risk Function is not fully informing in formulation of corporate strategy

Recommendations & actions	Gaps addressed
1. Incorporate reputational, vendor, model, and emerging risks (including but not limited to cyber risk) into all aspects of risk management. 2. Participate in formulation of business strategy from the outset. 3. Establish a resilient operating model for the Risk Function and processes; account for new risks in Insurer's business model and changing market competition and macroeconomic environment. 4. Define Risk Appetite at a more granular level for specific stakeholders (by line of business, product, and/or risk type); the appetite should be reviewed at least annually. Develop risk appetite for each of key risks – financial and nonfinancial, and advance it to setting the appetite at the product level in conjunction with the LoBs. 5. Develop and implement a cost allocation methodology. 6. Designate Risk Function as a client of the IT function. Provide business requirements to the IT Department to have appropriate functionality built into GRC Tool. Data management should be a key stakeholder in this execution. 7. Lead with technology to accelerate execution of risk operating model. The GRC tool should be leveraged for risk management, This is related to #6 above. 8. Review current resources to cover entire business both from number of individuals levels, and the required skill set within Risk Function. Identify all activities under Risk Function's umbrella. Allocate time and effort required for each activity. 9. Focus on demonstrable value through business partnership. 10. Evaluate business strategy in context of risk management and how the risk strategy is being operationalized. Interface this with the available capital (from Finance function) and also that is in sync with the corporate strategy.	• 1A – A formal risk strategy that lists the purpose/objectives, stakeholders, participants, interaction and linkage of Risk Function with outside units such as Global Risk, Finance, Businesses, Corporate Strategy is not well documented and not widely circulated. • 1B – While there is awareness of importance of link between business strategy and risk, it is not implemented effectively. • 1G – US risk appetite is set at a high level. • 2B – Business operations presents its risk to Risk Function; but due to lack of resources (and the associated skill set), Risk Function is not able to fully independently conduct assessment of operational, strategic and reputational risks comprehensively. • 2C – The Insurer organization is not nimble enough to be able to flex with the changing environment. • 3A – Risk Function costs are not allocated to businesses. • 6A – Risk Function is not informed of third-party risk in the organization (and not deeply involved in the program). • 6B – The GRC tool has had slow deployment.

Further considerations

- Risk Function should educate Leaders on need for Risk involvement in strategy development
- Risk Limits and Targets should be unambiguously articulated and form part of Risk Appetite Statement
- Escalate significance of businesses' participation in managing risk.

Items in dark blue font are prioritized recommendations and closing them will yield quick benefits and accelerate the establishment of a foundation to achieve an "Optimized" future state

Quantify Risk (*Illustration*)

Theme: Risk Function is not quantifying the risks that it is mandated to manage.

Recommendations & actions	Gaps addressed
1. Develop methodology and measures to quantify risk to include robust Stress Testing and Reverse Stress Testing program. Build a loss event database and quantify in a simpler scenario-based approach (which then should be subsequently enhanced). 2. Champion stress testing in the firm through Risk function. 3. Develop Recovery & Resolution Plans by Risk Function for the US business. This is achieved by succinctly defining roles and responsibilities of the Risk Function function. 4. Provide Risk Function the visibility and direct access to source risk data. Create a well-defined data governance function in Insurer. 5. Implement data governance - Champion the necessity of data management and data quality. 6. Consolidate quantitative risk data, not just as a register or listing but as an actual risk portfolio, to provide an overall view of the risks in the US business. 7. Identify key data elements and develop database of internal and external loss events pertinent to Insurer's business. 8. Create standard process to compute and quantify impact of, strategic and reputational risks on Insurer's capital, reserves, and its profitability (and risk-based profitability).	• Risk Function does not comprehensively participate in managing, strategic and reputational risks affecting US business; it also does not have active participation in Global Risk's Stress Testing program for these risks. • While not the owner of data, Risk Function does not have insight into quantitative data (including, but not limited to, data quality, data completeness, data accuracy, data transformation) for risk so data can be leveraged to improve the identification, assessment and reporting of risks. • Risk is not quantified. Assessment of risk is only based on a less precise qualitative, subjective, and judgmental approach. • Risk reporting is not informing of risks. • Risk Function participation in stress testing is limited. • The deployment of GRC tool at Insurer is moving slowly compared to its implementation at other organizations. Given the need to improve risk processes with help of technology, the benefits will be realized much later, while the need to make processes more effective and efficient is immediate.

Further considerations

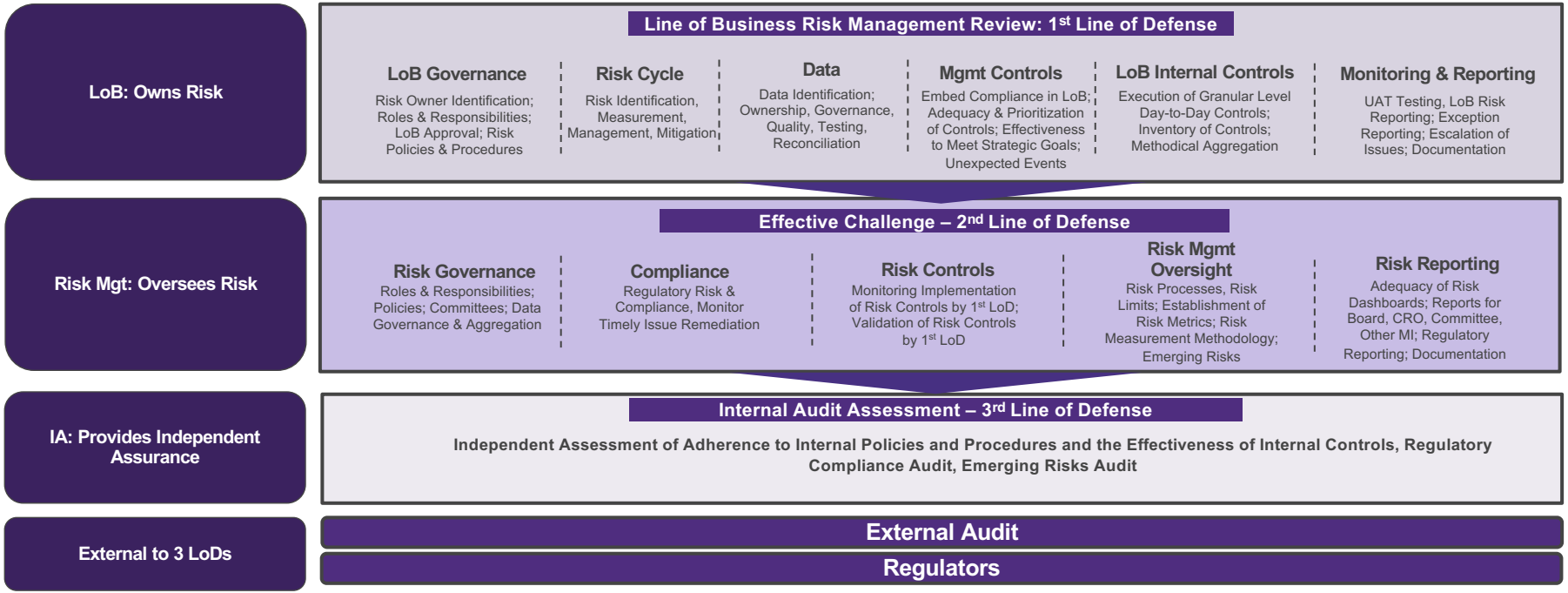
- Data governance initiatives will require senior management sponsorship
- The Risk Function needs to ensure metrics use are business metrics that have a real meaning to stakeholders
- Risk Function needs to educate Leaders on need for Risk involvement in strategy development

Items in dark blue font are prioritized recommendations and closing them will yield quick benefits and accelerate the establishment of a foundation to achieve an "Optimized" future state

Artifact 1:
Risk Governance

This section presents a recommendation of the 3 LoD structure for Insurer's Risk Function

Risk governance: Three Lines of Defense

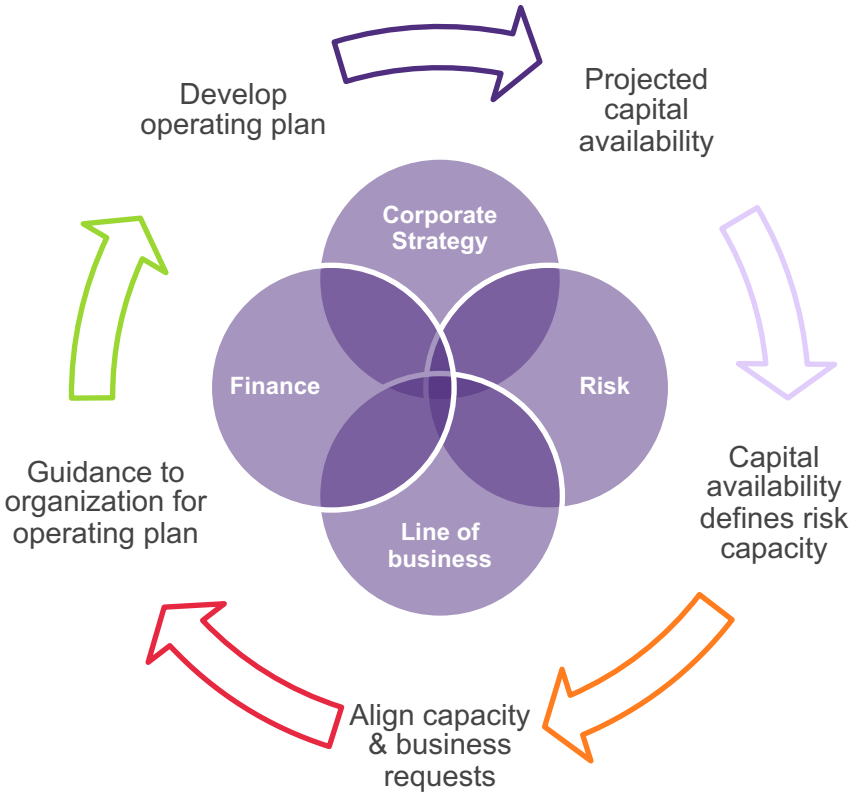


Artifact 2:
Risk Appetite Life Cycle

This section illustrates the linkages between the key functions of an insurer's business – strategy (through strategic plan), risk (through risk appetite and capacity), line of business (through aligning risk capacity and execution) and finance (through a capital plan). It also lists the need for blending top down and bottom-up approaches in execution.

Linking Corporate Strategy, Risk, Finance and Business

Illustrative for Insurer's business



Integrate Corporate Strategy, Capital Plan and Risk Appetite into Business Planning

Blend Top-Down Approach (strategy, guiding principles, risk philosophy) with Bottom-Up Approach (quantitative measures at portfolio/product level)

Issue Risk Management guidance for businesses by risk type (e.g., for operational, strategic, reputational risks)

Artifact 3:
Regulatory Considerations

This section illustrates a note on regulatory mindset in assessing risk governance and risk culture of an insurance company which is also applicable to Insurer.

Regulators

- In the US
  - No federal insurance regulator
  - Managed via proxy through NAIC
  - State Regulations
  - Required
    - Capital (Risk Based Capital, AM Best, Economic Capital)
    - Pricing (why are insurers abandoning – not risk based pricing)
  - Where is ESG?
- In Europe
  - Solvency II Rule rules

There have been seismic shifts in regulatory approach by the NAIC and Insurance Departments

- Retrospective → ***Prospective***
- Company → ***Enterprise***
- Financial Statement → ***Governance***
- Rules → ***Principles***
- Getting to know the DNA of the company
- Regulatory are expecting more Board involvement in this new regulatory approach
- Is management ready?

Artifact 4:
Educational Sources

This section lists select sources of reading for understanding risk management in the insurance industry. It also lists the certification course for insurance risk managers.

Educational Sources

- Have you ever read
  - NAIC's White Paper on High Level Corporate Governance Principles
  - NAIC's Comparative Analysis of Existing U.S. Corporate Governance Requirements
  - NAIC's Model Corporate Governance Manual Disclosure Model Act and Model Regulation
  - Exhibits L & M on the NAIC's Financial Examiners Handbook
    - Exhibit L – Branded Risk Classification
    - Exhibit M – Understanding the Corporate Governance Structure
  - Form F – Enterprise Risk Report
  - NAIC's Own Risk and Solvency Assessment Guidance Manual
  - NAIC's Own Risk and Solvency Assessment Feedback Pilot Project Observations
  - Financial Risk Manager certification materials from Global Association of Risk Professionals
  - Gartner
  - Risk.net

- Select certification courses recommended for the insurance risk practitioners
  - Certified Risk Manager (CRM) administered by The National Alliance for Insurance Education & Research
  - RIMS – Certified Risk Management Professional (RIMS-CRMP) accredited by the American National Standards Institute
  - Certified Fraud Examiner (CFE) administered by Association of Certified Fraud Examiners

END