KPMG

cutting through complexity

Risk & Regulatory Series

Market Conduct

Market Conduct

– Background

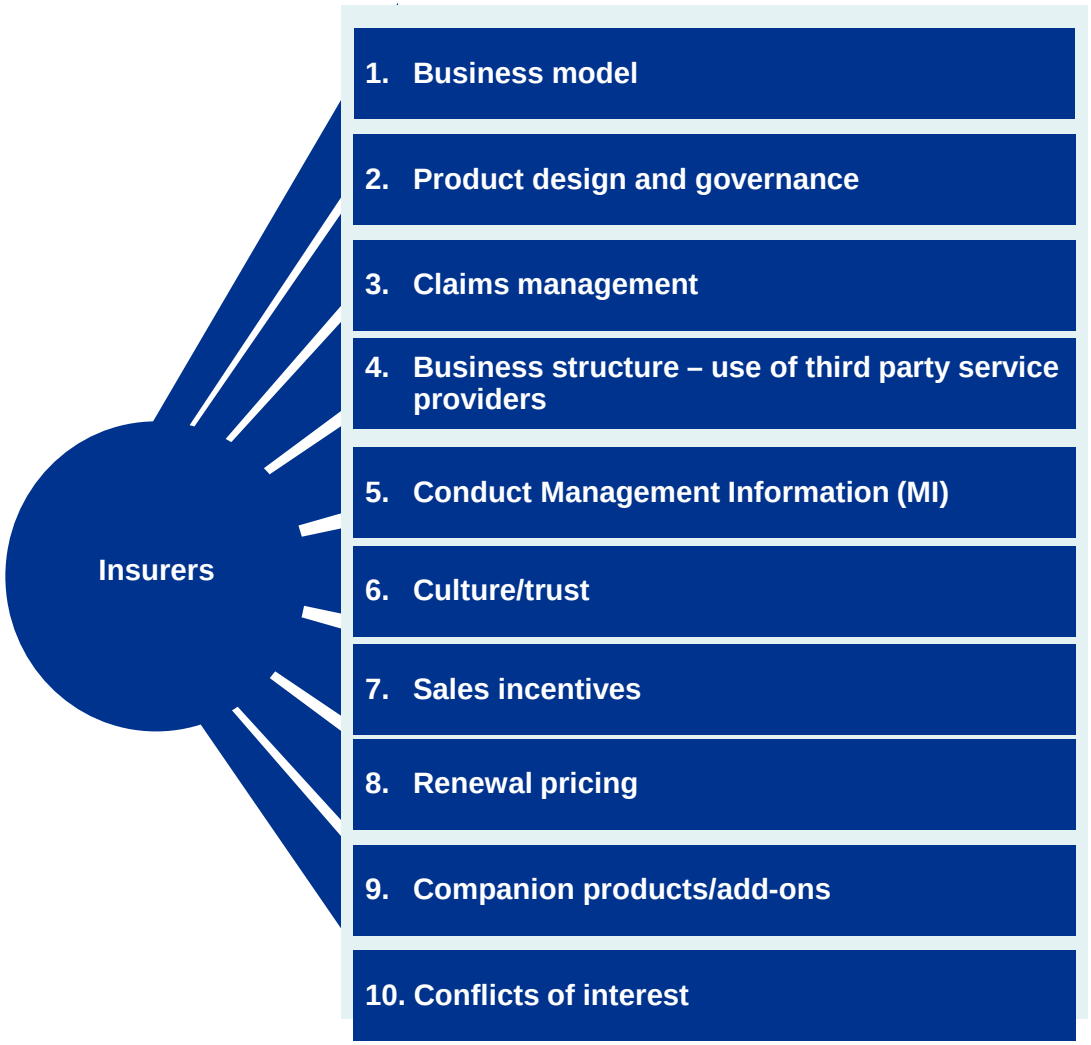
Market Conduct Risk – Overview

- Conduct risk is “the risk of regulatory censure and/or a reduction in earnings/value, through financial or reputational loss, from inappropriate or poor customer treatment
- Issues:
  - A shift from caveat emptor - no longer enough for insurance companies to leave customers to evaluate product options and make purchase decisions in a vacuum
  - Regulatory and customer expectations are changing
  - Risk may not be well understood by the organization
  - Costs of compliance are rising
  - Current frameworks may not be adequate
  - Companies need to invest in conduct risk mitigation
  - Insurers which are part of international groups may need to also comply with HO/foreign regulators expectations
- What do insurance companies have to do?
  - Operationally transform systems, processes, and controls
  - Across-the-board cultural change

Conduct Risk Characteristics

- Aggregation of many events, most small ticket items, some not
- High probability
- Distinction between misconduct and detriment with time lag between them
- Scale of detriment may be contingent on market movements: should that affect how severely behaviour is viewed?
- Waterbed effect: clearing up one issue may just move the problem if incentives not fixed
- Impact of the same monetary loss different for different consumers
- Potential for multiple risks to accumulate in the financial institution

Illustrative Areas of Conduct Risk for Insurers



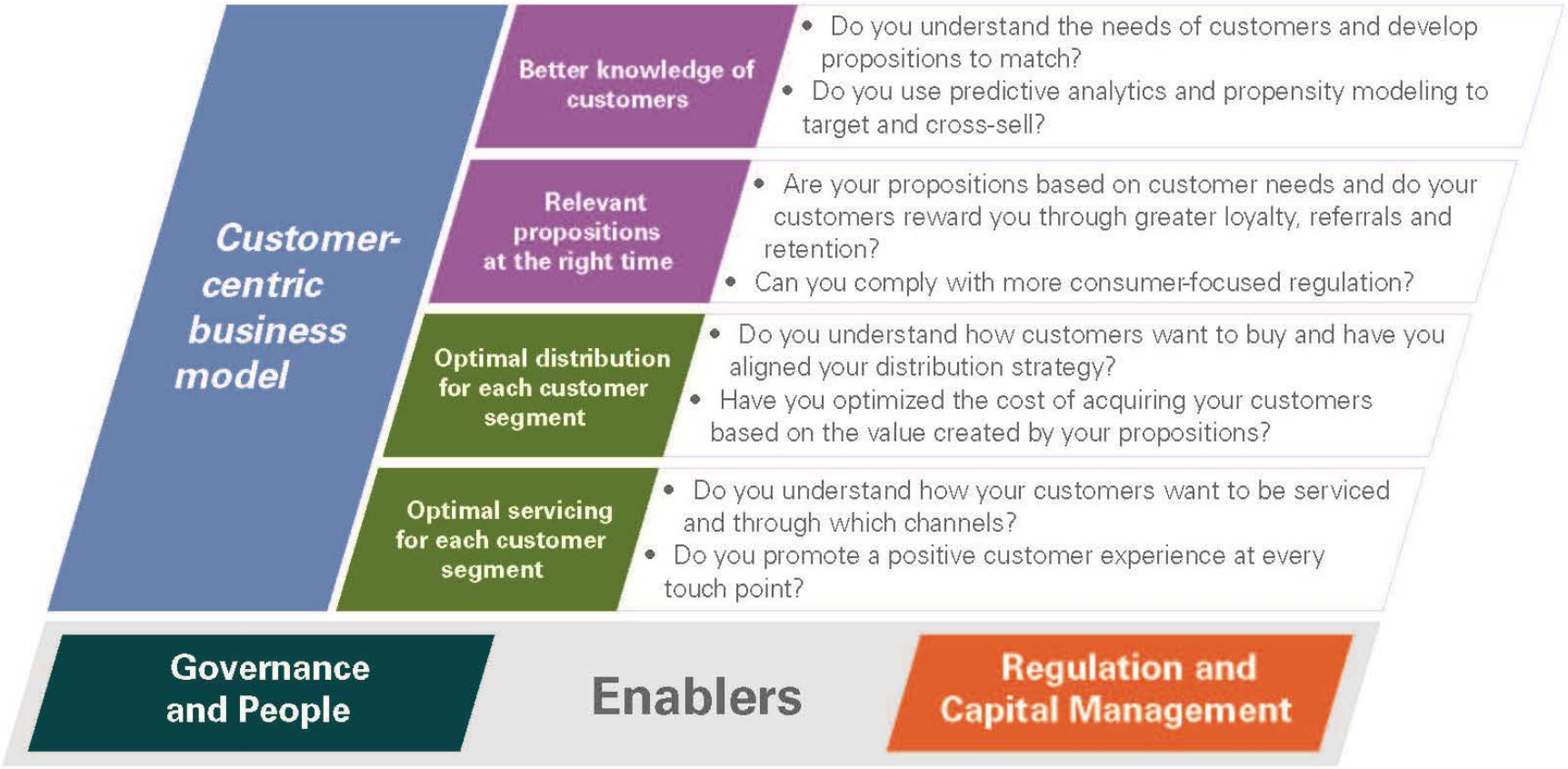
Not understanding the elements of Conduct Risk and mitigating the risks with a robust Control Risk Management System, can put the insurer at great risk of conduct failures

Source: Financial Conduct Authority

Providing a Differentiated Customer Experience

Customer-Centric Business Model

Components of a customer-centric business model



Source: The Valued Insurer, KPMG International, 2013

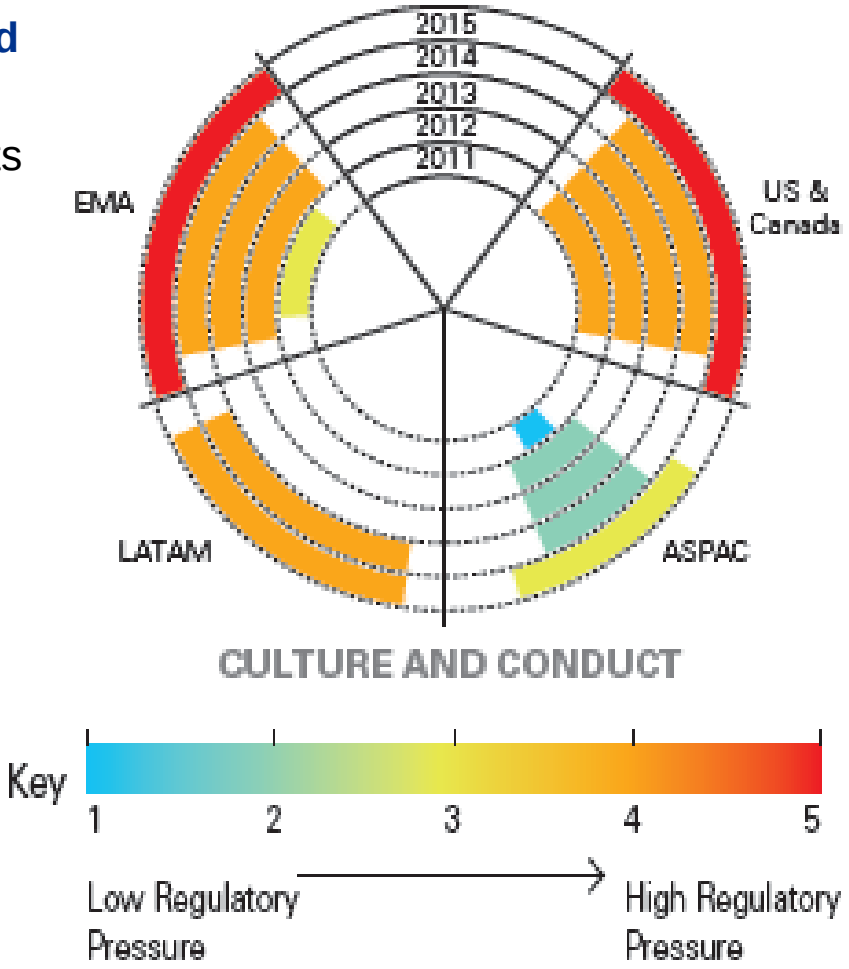
OECD Consumer Protection Principles – 2011

1. Financial consumer protection should be an integral part of the legal, regulatory and supervisory framework.
2. There should be oversight bodies explicitly responsible for financial consumer protection, with the necessary authority to fulfil their mandates.
3. All financial consumers should be treated equitably, honestly and fairly at all stages of their relationship with financial service providers.
4. Financial services providers and authorized agents should provide consumers with key information that informs the consumer of the fundamental benefits, risks and terms of the product.
5. Financial education and awareness should be promoted by all relevant stakeholders and clear information on consumer protection, rights and responsibilities should be easily accessible by consumers.
6. Financial services providers and authorized agents should work in the best interest of their customers and be responsible for upholding financial consumer protection. Relevant mechanisms should protect consumers' deposits, savings, and other similar financial assets, including against fraud, misappropriation or other misuses.
7. Consumers' financial and personal information should be protected.
8. Consumers should have access to adequate complaints handling and redress mechanisms.
9. Nationally and internationally competitive markets should be promoted in order to provide consumers with greater choice among financial services and create competitive pressure on providers to offer competitive products, enhance innovation and maintain high service quality.

Regulatory Developments

Examples of material market conduct failures and their corresponding impact on institutions:

- Insurer (UK): Failed to take steps to ensure that its customers were being treated fairly. FCA was of the view that customers were taking out accident insurance products they did not understand.
  - Fine/loss: £8.3 million
- Top 5 Insurer (US): Market conduct issues and churning.
  - Fine/loss: $2 billion US in restitution
- UK Banks: Selling payment protection insurance products, which were either not needed, already covered or not disclosed.
  - Fine/loss/restitution: £ many billions
- Bank owned insurer (UK): Breached rules on handling customer complaints
  - Fine/loss : £2.1 million



Source: Pressure Index (from KPMG 2015 International Survey)

International Association of Insurance Supervisors – Insurance Core Principles

What is in the ICPs affecting market conduct?

ICP 19 – Conduct of Business
Ensure customers are treated fairly, before a contract is purchased, through to fulfillment of contract obligations
Policies and procedures for product development and marketing, providing clear information on rights and obligations
Ensuring fair treatment is embedded in governance, management, processes and organization culture
Ensuring product suitability to customer circumstances, managing reasonable expectations of customers
Ensuring high quality advice, and management of conflicts of interest

Response of Canadian Authorities to 2014 IMF FSAP report:

> "*The introduction of ICPs dealing with market conduct issues is relatively new. As a result there is a learning curve to understand how the IMF contemplates that specific standards should be implemented. As the ICPs and assessment techniques evolve, it will be important to balance consideration of process with consideration of outcomes achieved. Past experience has not demonstrated a history of significant unaddressed market conduct problems in Canada.*"

Canadian Regulatory Developments

Canadian Council of Insurance Regulators

- Work plan in place for a new Cooperative Market Conduct Supervisory Framework to assist CCIR member jurisdictions to improve their compliance with the International Association of Insurance Supervisors (IAIS) Insurance Core Principles (ICPs).
- Development of inter-jurisdictional agreements, or MOUs, and a Supervisory Framework that to hopefully be adopted by all member jurisdictions.
- Potential consultations with industry.

Ontario – Mandate Review of FSCO

- *"Should the legislated mandates of the agencies explicitly refer to the goal of consumer protection, and should that goal be balanced with the goal of promoting a strong financial services sector? If yes, how?"*

Market Conduct

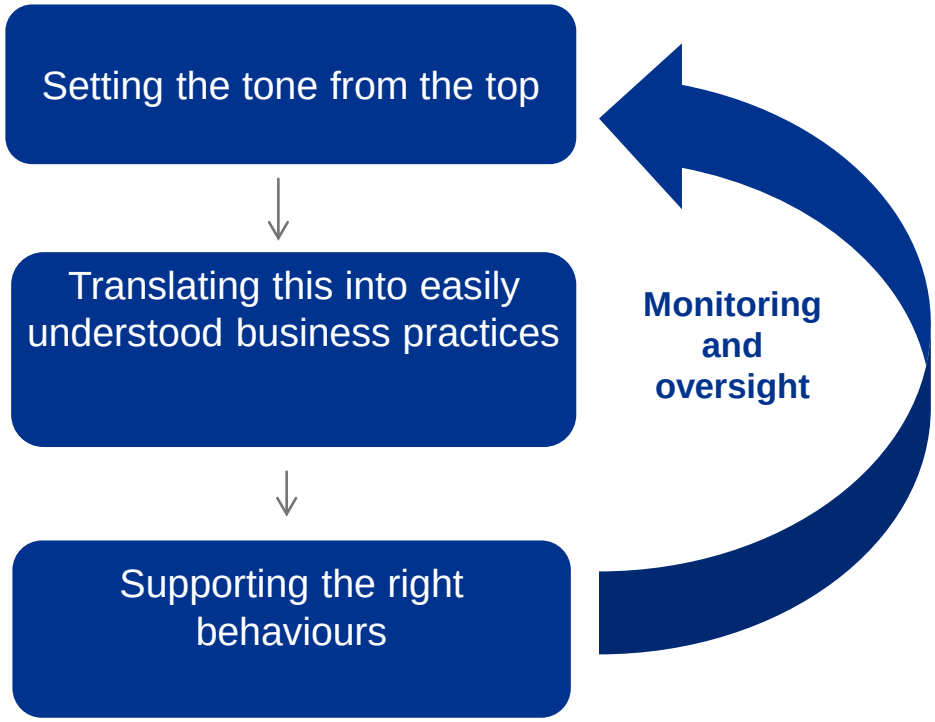
– Risk Management Framework

Conduct Risk Management Framework

Below is an illustration of a set of elements under a Conduct Risk Management Framework:

Role of Risk Culture

Key drivers of culture at a firm



Both regulators (PRA and FCA), the approach – and the desire to tackle root causes – places increasing emphasis on how firms are run and their culture

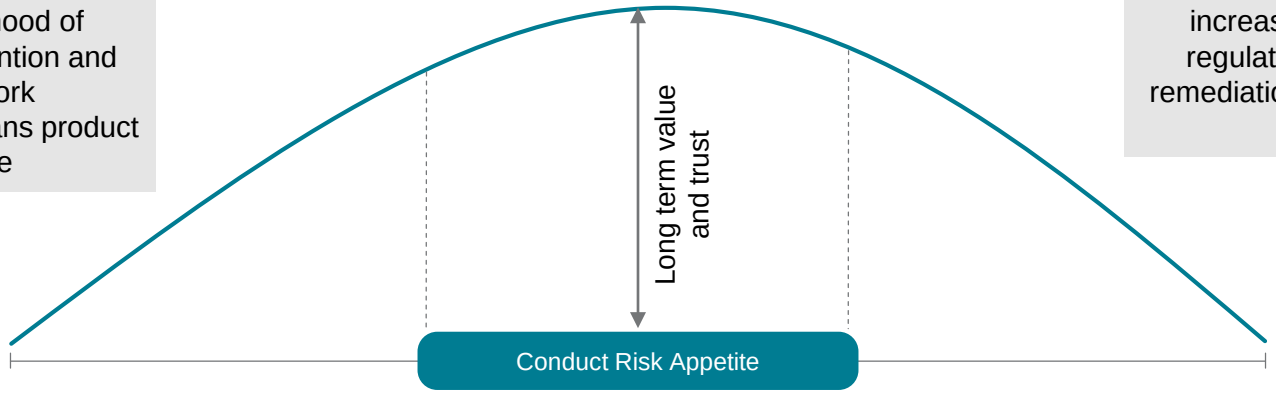
"An effective culture is on that supports a business model and business practices that have at their core, the fair treatment of customers and behaviours that do not harm market integrity"

FCA, April 19, 2014

Conduct Risk Appetite

Reduced/No profits
'Too expensive'
Reduced likelihood of regulatory intervention and remedial work
Cost of control means product is unviable

Short term high profits
Historic data suggests increased likelihood of regulatory intervention, remediation and reputational risk



Zero Risk Tolerance

'Too Risky'

Potential Conduct Risks Areas

- Market/environment
- Proposition/brands
- Clients
- Core Business Processes
- Operations and Infrastructure
- People and culture

Data Analytics – the Caution

- Applying data analytics to understand and refine and further target products and service to specific customer groups will speak to customer needs and expectations. However, offerings can become so specialized that the overall process is extremely difficult to administer, leading to mistakes, inaccuracies, unintended conduct issues, and regulatory risks.
  - In many cases, the systems and process back-office infrastructure within the institution is not necessarily designed to support this level of customization.
  - This complexity is compounded by the fact that a large portion of support and processing functions are outsourced, to third parties making it difficult to align those outsourced tasks with customer commitments and regulatory expectations.

Need to look at the end-to-end impacts when using Data Analytics – the Marketing and Sales Front-End and the Back-Office Infrastructure

Requirements for Addressing Customer Complaints

Customer complaints are expressions of dissatisfaction with any aspect of a company's operations, which has a direct impact on customer satisfaction/experience, revenues, operational costs, and organizational risk.

Based on KPMG's engagement experience, complaints fall into two categories:

- **Formal Complaints:** Is the process of a customer reporting a bad experience with a service, interaction or disagrees with a problem resolution and reports the concern to the company (i.e. call center, web, executive office, in person) or a third party (FCAC, FSCO, better business bureau, etc.)
- **Informal Issues:** Are informal complaints reported by customers that occur when a problem arises during the coarse of normal activities/transactions.

Complaints Management is the ***strategy, processes and enabling tools to proactively eliminate and rapidly respond to customer problems across levels of severity.***

Conduct Management Information – Today

THE PROBLEM WITH CONDUCT RISK INFORMATION TODAY

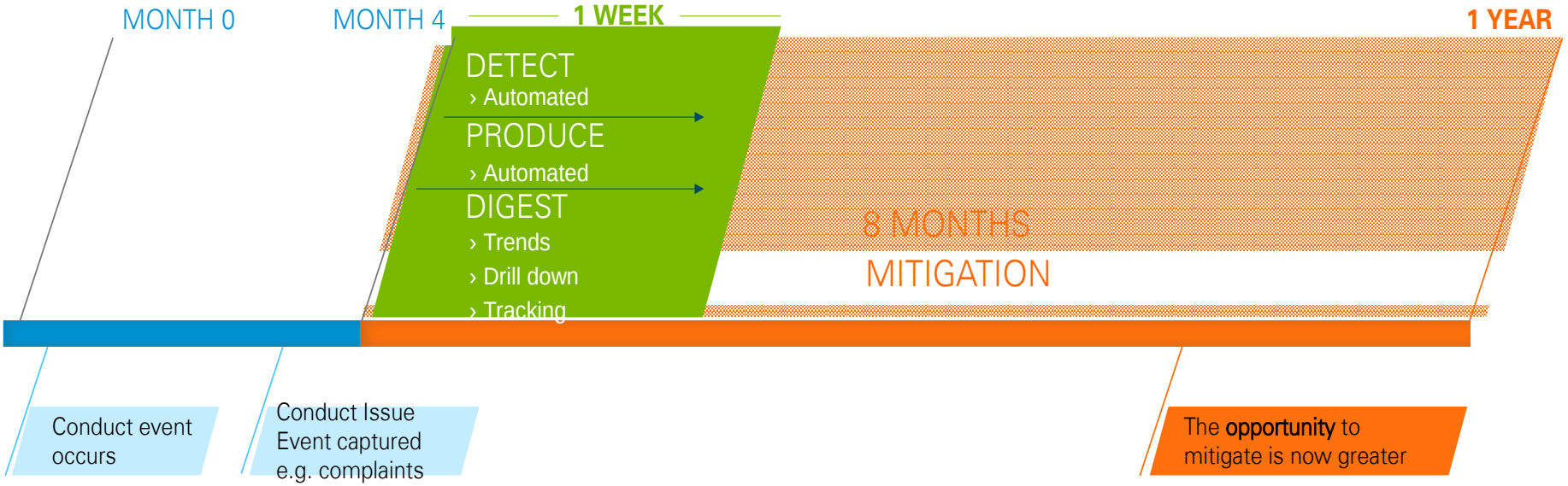
- / Manual collation of static reports
- / Cleaning data
- / Little time spent on analysis
- / Conduct Issue Events based on data that is at least two months old

Conduct Management Information – Where is it Heading?

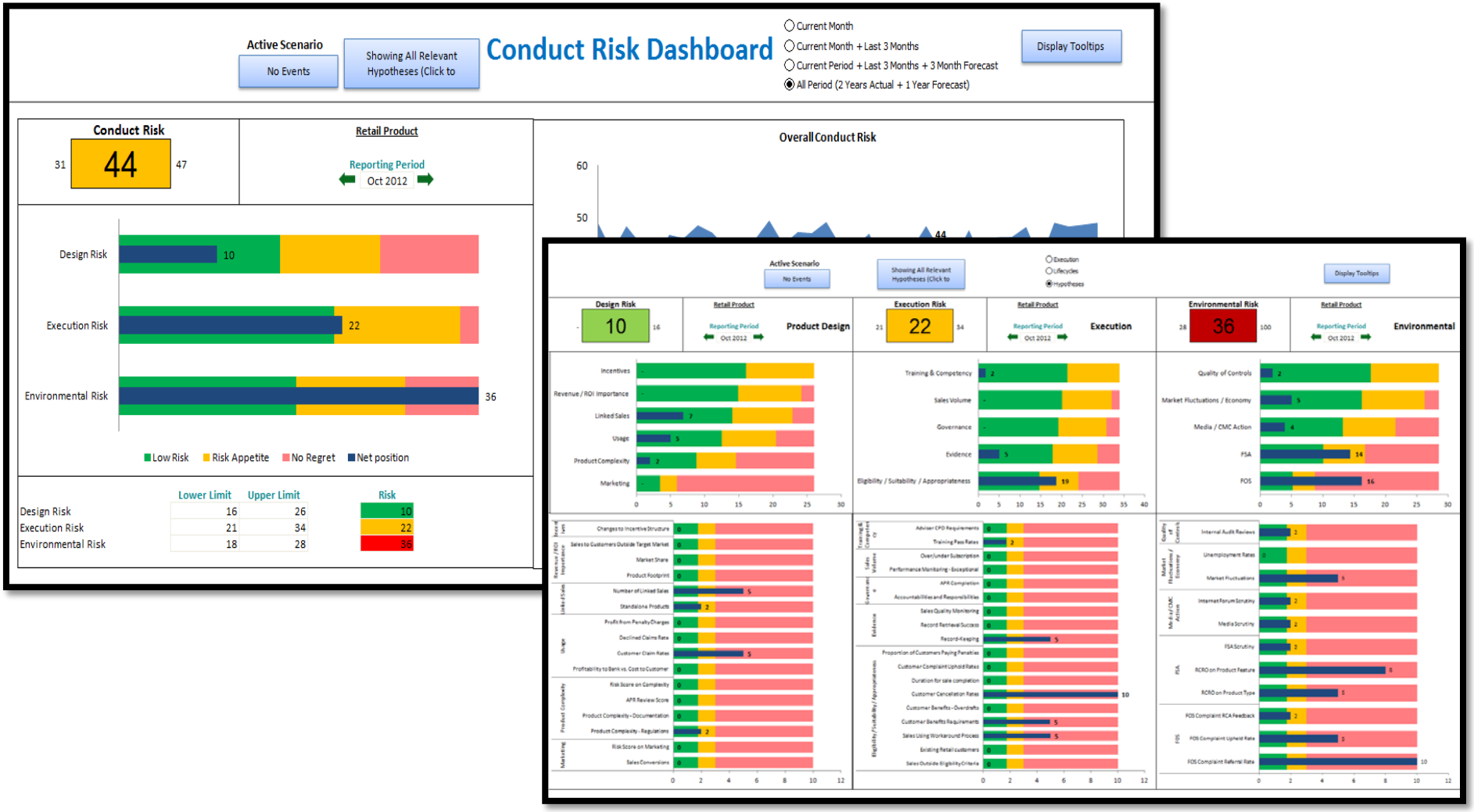
CONDUCT RISK INFORMATION FUTURE STATE – helps ensure that products and services provide value to customers and generate legitimate profits

- / Continual improvement and Conduct Issue Events analytics
- / Identifies new lead indicators and more tailored thresholds
- / leading to earlier detection

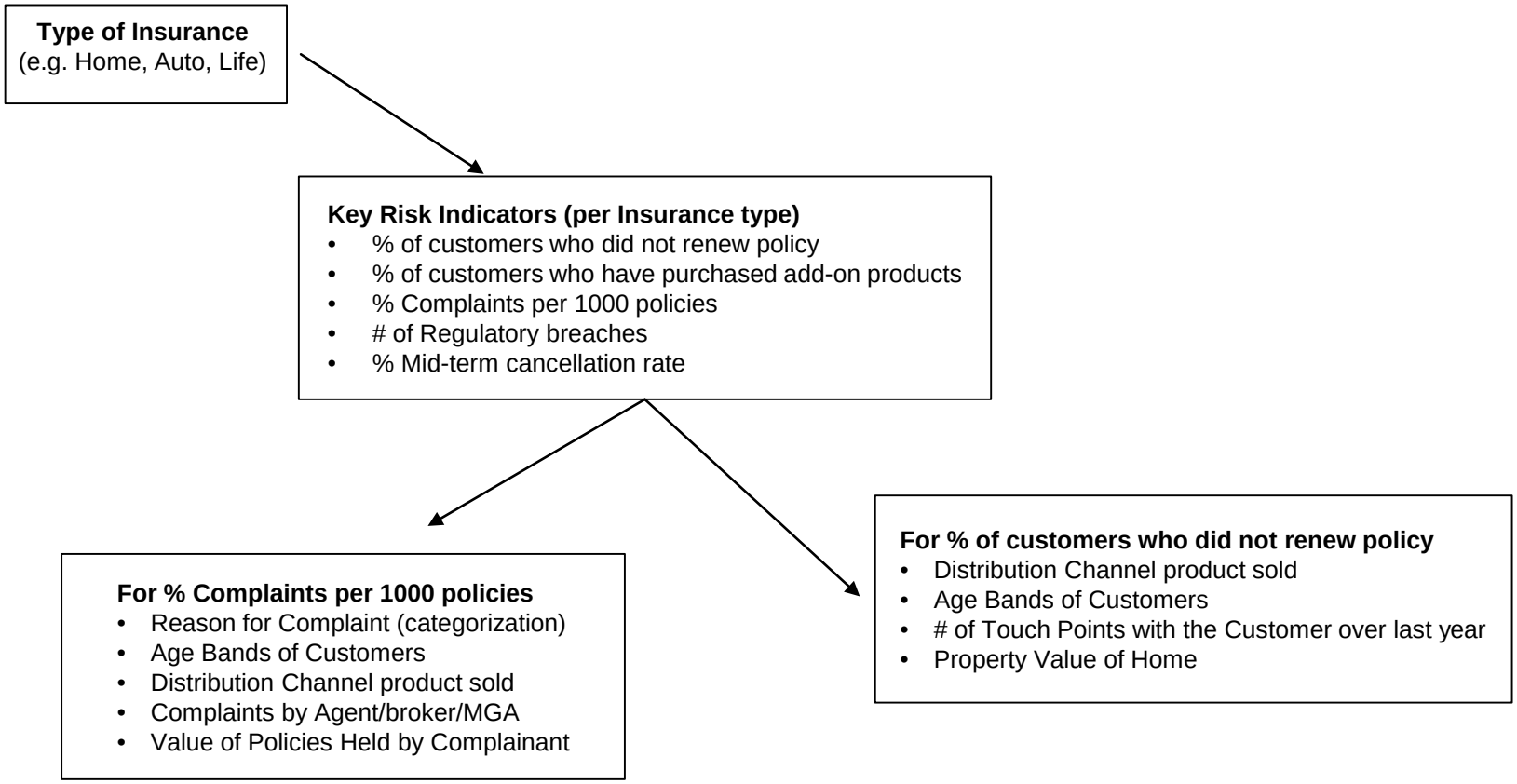
- / Drill down to route issues
- / Remediation recommendations
- / Assigned actions
- / Tracking improvements
- / Evidence based enhancement to capturing Conduct Risk Events



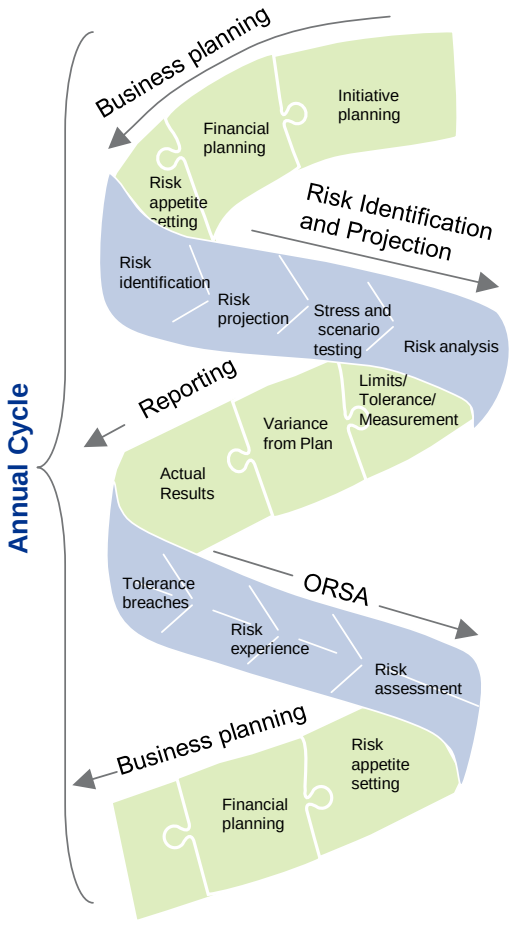
Leading Edge Conduct MI



Leading Edge Conduct MI (illustration of a set of drilldown analytics)



Conduct Risk Needs to be Incorporated Into the ORSA Process



Functions/activities
Risk, Finance (incl. Actuarial), Operations (incl. strategy), Boards/Committees

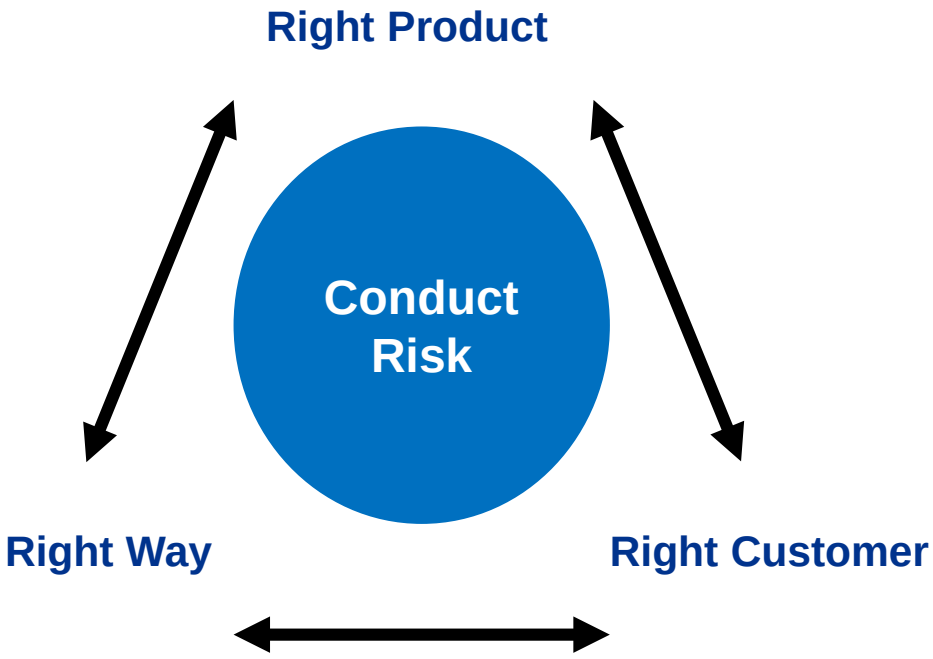
1. Inputs	2. ORSA process steps key activates	3. Outputs
▪ Risk monitoring ▪ (strategic) risk identification ▪ SCR calculation	**Risk identification**	▪ Current qualitative risk profile ▪ Current quantitative risk profile
▪ Strategy and business plan ▪ Base scenario	**Risk projection**	▪ Projected risk profile
▪ Risk scenario's ▪ Strategic risk identification	**Stress and scenario testing**	▪ Overview impact stress testing
▪ Strategy and business plan ▪ Base scenario ▪ Risk appetite	**Risk analysis**	▪ Analysis of the current and projected risk profile in relation to the business plan (strategic objectives, financial plan and risk appetite) ▪ Statement on the appropriateness of the Risk and Capital Management system

ORSA Report

Stakeholders
Board/Committees, External stakeholders, Business functions

Closing Thoughts

The 3 Simple Rights to Conduct Risk



Objective: ensure products provide value to customers and generate legitimate profits

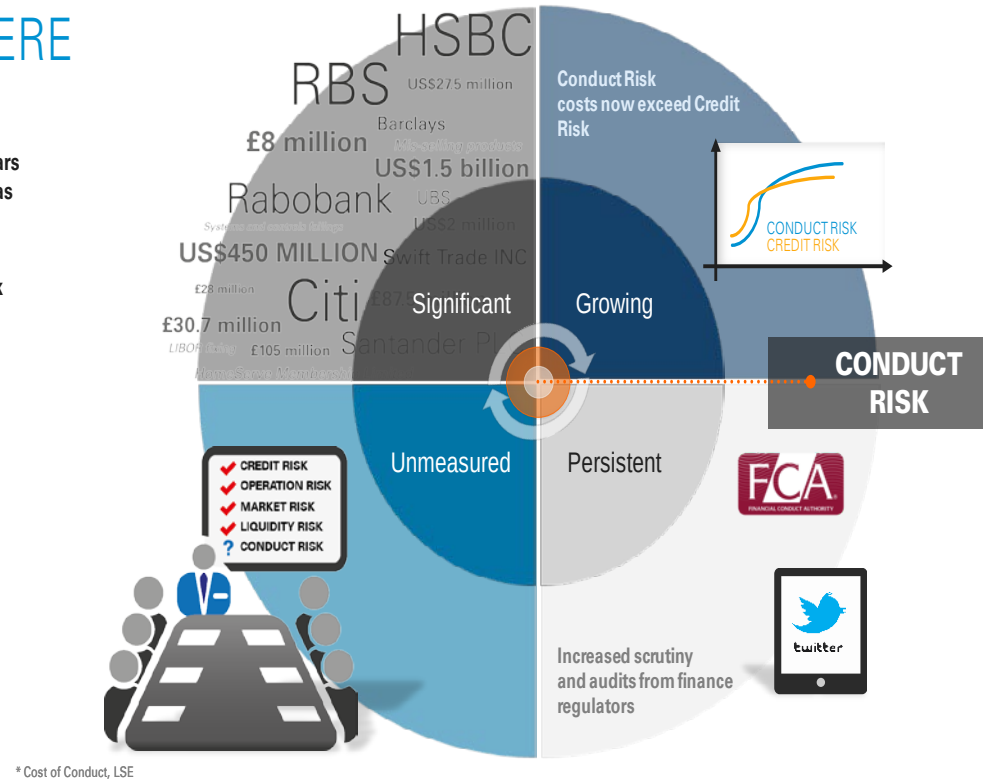
Closing Thoughts

Conduct Risk: ***"the risk of a firm treating its customers unfairly and delivering inappropriate outcomes".***

Conduct Risk puts the Customer at the heart of the business.

CONDUCT RISK IS HERE TO STAY

- Over the past five years a new view of Risk has emerged
- Not the risk from the customer, but the risk to them



* Cost of Conduct, LSE

Other Presentations

The other presentations that were presented as part of the Risk and Regulatory series are:

- IFRS 9 Classification, Measurement and Impairment (Insurance Sector): Initial Considerations
- The New World of Cyber Resiliency
- ORSA – Next Steps
- Regulatory Compliance Management

Presenters

Elizabeth Murphy
Partner
Financial Risk Management
T: +1 416-777-8279
E: elizabethmurphy@kpmg.ca

David Pelkola
Director
Financial Risk Management
T: +1 416-777-8761
E: dpelkola@kpmg.ca

cutting through complexity

KPMG

cutting through complexity

Risk & Regulatory Series

Regulatory Compliance Management

Agenda

I. **OSFI Guideline E-13 Regulatory Compliance Management ("RCM")**

   – Insights into OSFI Guideline Key Elements

II. **RCM versus earlier Legislative Compliance Management ("LCM")**

III. **Potential RCM Issues seen in practice**

IV. **Conclusion**

I. OSFI Guideline E-13: Regulatory Compliance Management

RCM FRAMEWORK – OVERVIEW

OSFI's expectations regarding a FRFI's RCM framework include:

- Should enable a FRFI to apply a risk-based approach to identify, risk-assess, communicate, manage and mitigate regulatory compliance risk.
- Should be reviewed and updated regularly to address any need for improvement, new and changing regulatory risks, new business activities and any changes to corporate structure.
- Roles and responsibilities of all individuals involved in the assessment and management of regulatory compliance risk should be clearly documented.

OSFI will assess the quality of the RCM framework at two levels of control:

1. Operational management for a given business activity used to manage risk on a day-to-day basis.
2. Ongoing enterprise-wide oversight of day-to-day compliance controls by individuals or oversight functions that are independent of the activities they oversee.

I. OSFI Guideline E-13: Insights into Key Elements

RCM FRAMEWORK – KEY CONTROL ELEMENTS

1. Role of the Chief Compliance Officer

- Overall responsibility for compliance should be assigned to a member of Senior Management who should be designated, at least functionally, as the Chief Compliance Officer (“CCO”).
- OSFI recognizes that this individual may have other responsibilities as well, especially in the case of small, less complex FRFIs.
- The CCO should:
  - Not be directly involved in a revenue-generating function or in the management of any business line or product of the FRFI
  - Have sufficient stature and authority within the FRFI to influence the FRFI’s activities
  - Have a clearly defined and documented mandate, sufficient resources, unfettered access, and for functional purposes, a direct reporting line to the Board (or relevant Committee of the Board)
  - Be responsible for ensuring on an ongoing basis that day-to-day RCM controls are sufficiently robust to achieve compliance with all applicable regulatory requirements enterprise-wide.

I. OSFI Guideline E-13: Insights into Key Elements

2. Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements

- Procedures
  - Ensure that appropriate individuals are provided with current and accurate information, which is updated as necessary to reflect new and changing regulatory requirements, as well as changes in products/services, strategic plans, corporate structure, and other activities.
  - Resources should be allocated and/or approaches determined under the RCM Framework using a risk-based approach.

I. OSFI Guideline E-13: Insights into Key Elements

2. Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements

- Identify the Inventory of Regulatory Requirements
  - A FRFI will often engage the services of external legal counsel or use a subscription service to provide a listing of regulatory requirements potentially applicable to the FRFI's business and to be considered as part of the RCM framework. All regulations impacting a FRFI, and not just the traditional Insurance Act/OSFI financial focused regulations, must be reviewed and included where appropriate.
  - Each regulatory requirement within the inventory should be reviewed by Compliance and assigned to a member of Senior Management, who will, in connection with Compliance and Legal, assess the risk associated with the requirement, design controls to mitigate the identified risk, as well as conduct and report the results of day-to-day monitoring and testing procedures.
  - Important that the inventory is reviewed and updated generally annually, and whenever there are regulatory changes or business changes (e.g. product/service, system or process) that could have regulatory impacts.
  - Relevant regulatory requirements then need to be mapped to the applicable business units within the FRFI. This results in a map of what regulatory requirements actual apply to the specific business units.

I. OSFI Guideline E-13: Insights into Key Elements

2. Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements

- Regulatory Risk Assessment Models
  - Regulatory requirements should be assessed using a standard and documented methodology which considers both the likelihood of increased inherent regulatory risk and impact of not meeting the regulatory requirement. Often a weighting approach is used which factors Likelihood and Impact.
  - Illustrative **Likelihood** factors: (1) Volume and Scale of Activity, (2) Complexity of Regulation, (3) Newness of Requirement, and (4) History of Regulatory Issues.
  - Each **Likelihood** element is scored on a three level scale – High, Medium and Low – and averaged to indicate the likelihood of regulatory issues potentially impacting the FRFI.
  - **Impact** reflects the potential financial loss or business sanctions, personal liability to employees or directors, or reputational and business damage due to a regulator's or the press ability to publish violations in the event of non-compliance.
  - **Impact** is scored on a 3 level scale – High, Medium and Low and linked to the Likelihood score to create a directional composite regulatory risk score for the lines of defense to use in their planning.

I. OSFI Guideline E-13: Insights into Key Elements

2. Procedures for Identifying, Risk Assessing, Communicating, Managing and Mitigating Regulatory Compliance Risk and Maintaining Knowledge of Applicable Regulatory Requirements

- Mapping of Regulatory Requirements to Business Units and Risk Assessed
  - In practice, the RCM Inventory of Regulatory Requirements would be at a more detailed level below the Regulation Name. A similar exercise would be completed mapping the regulatory requirements to business units and the regulatory requirements would be risk assessed to focus control, monitoring and testing efforts.

Illustrative

	Business Units				Regulatory Risk Model Factors					
Regulation Name/ Description	**Business Unit A**	**Business Unit B**	**Business Unit C**	**Finance**	**Volume and Scale of Activity**	**Complexity of Regulation**	**Newness of Requirement**	**History of Regulatory Issues**	**Impact**	**Directional Composite Regulatory Risk Rating for Business Unit Consideration**
Complaint Regulations	X	X			High	Medium	Medium	High	Medium	Medium-High
The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)	X	X	X	X	High	High	Medium	High	High	High
Personal Information and Electronic Documents Act (PIPEDA)	X	X		X	High	Medium	Low	Medium	High	Medium-High
Canada Anti-Spam Legislation (CASL)				X	High	Medium	High	Medium	Medium	Medium
OSFI Guideline B-10 Outsourcing of Business Activities, Functions and Processes	X	X	X	X	High	High	Low	High	Medium	Medium-High

OSFI Guideline E-13: Insights into Key Elements

3. Day-to-Day Compliance Procedures (in First Line of Defense)

- Monitoring and Testing
  - Each identified regulatory requirement needs to have a corresponding control that is designed and operating to mitigate the regulatory risk. The best scenario is when these regulatory related controls are integrated into and are seen as business as usual processes.
  - Ongoing business unit testing should be instituted that covers both the design and operating effectiveness of the controls to mitigate regulatory risks identified for that process.
  - Any issues noted should be reviewed by the corresponding accountable member of Senior Management, with action plans noted and remediation progress tracked.

Illustrative

Regulatory Requirement		Control Assessment									Management Response	
Requirement ID	Requirement Long Description	Control ID	Control Statement	Department Performing the Control	Accountable Individual	Control Type	Control Design Rating	Control Design Observation	Control Operating Effectiveness Rating	Control Operating Effectiveness Observation	Action Plan	Remediation Status

I. OSFI Guideline E-13: Insights into Key Elements

4. Independent Monitoring and Testing Procedures (in Second Line of Defense)

- Adequacy and effectiveness of, and adherence to, day-to-day compliance procedures including monitoring and testing procedures, should be independently monitored and tested on an ongoing basis by an appropriate oversight function, such as Compliance and the Chief Compliance Officer (CCO).
- Employ a risk-based approach (i.e. high risk tested more frequently and in more depth).
- Methodology should be sufficiently consistent enterprise-wide to enable the aggregation of information to identify any patterns, themes or trending in compliance controls that may indicate weakness.
- Include the verification of key elements of pertinent information used in key reports.
- Note: The CCO's independent monitoring and testing generally involves a combination of: (1) reviewing the business unit's testing results and (2) executing independent examination and re-performance of regulatory controls to validate their design and operating effectiveness.

Internal Audit or other independent review function is expected to validate the effectiveness of, and adherence to, the RCM framework enterprise-wide by risk-based testing on a rotational or other regular basis that the Board considers appropriate. This includes testing of both operational and independent oversight levels of compliance control. The scope should include consideration of material regulatory risks and their corresponding controls.

I. OSFI Guideline E-13: Insights into Key Elements

5. Internal Reporting

a. Reporting Procedures

- Ensure that sufficient pertinent and reasonably verifiable information about RCM adequacy and effectiveness is communicated on a timely basis to individuals with RCM responsibilities.
- Should include:
  - Aggregation of monitoring and testing results within and across areas of business activity pertinent to the RCM responsibilities of the report recipients; and
  - Regular reports to Senior Management and the Board or Committee(s) of the Board, in a manner and format that:
    i. Allows them to clearly understand the risk to which the FRFI is exposed and the adequacy of key controls to manage that risk; and
    ii. Facilitates the performance of their oversight responsibilities.

I. OSFI Guideline E-13: Insights into Key Elements

5. Internal Reporting

b. Compliance Reports to Senior Management and the Board or Committee(s) of the Board

- RCM reports should be made on a regular basis (at least annually) and approved by the Board.
- Such reports should cover:
  - Results of enterprise-wide compliance oversight, including:
    i. Material RCM framework weaknesses
    ii. Instances of material non-compliance
    iii. Material exposure to regulatory compliance risk (and their potential direct or indirect impact on the FRFI)
    iv. Related remedial action plans.
  - Information that may assist the Board in its decision-making about strategic direction and controls, for example:
    - Significant legislative and regulatory developments
    - Industry compliance issues
    - Emerging trends and regulatory risks.

I. OSFI Guideline E-13: Insights into Key Elements

5. Internal Reporting

b. Compliance Reports to Senior Management and the Board or Committee(s) of the Board (Continued)

- As part of internal compliance reporting, the CCO should:
  - Establish the general areas of content addressed in, and frequency of, regular RCM reports made to the CCO by operational management. This should be sufficient to enable the CCO, Senior Management and the Board to discharge their RCM responsibilities;
  - Have a process in place to assess the accuracy and effectiveness of RCM information or analysis provided by business areas;
  - Meet with the Board on a regular basis, including, as appropriate, in-camera sessions; and
  - Provide an opinion, that is verified or easily verifiable, on a regular basis, but at least annually, to the Board on the adequacy and effectiveness of the RCM framework, and whether, based on the monitoring and testing performed by the Compliance oversight function, the FRFI is in compliance with applicable regulatory requirements.
- As part of internal compliance reporting, the Board should review the type, content and frequency of reports it will receive to ensure that it receives information that is necessary to carry out its oversight role.

I. OSFI Guideline E-13: Insights into Key Elements

5. Internal Reporting

c. Internal Audit or Other Independent Review Function Reports to Senior Management and the Board or Committee(s) of the Board

> *Internal Audit or other independent review reports to the Board should include sufficient pertinent information to facilitate the Board's periodic reassessment of the RCM framework, while maintaining their independence.*
>
> *These reports should assist the Board in assessing the reliability of RCM assurances provided by Compliance and Senior Management, and should be provided on a frequency that is approved by the Board.*
>
> *Significant review findings and recommendations for correcting deficiencies along with management's undertakings with respect to remedial action should be reported, as appropriate, to operational management, Senior Management and the Board.*

- Actions taken in response to significant recommendations should be monitored by operational management, Senior Management, and the Board.

I. OSFI Guideline E-13: Insights into Key Elements

6. Role of Internal Audit or Other Independent Review Function

- Verify and validate the design and operating effectiveness of, and adherence to, the RCM framework, taking into consideration the work of the Compliance oversight function, if appropriate.
- Scope of work routinely undertaken should include consideration of:
  - Reliability of the RCM framework
  - Management's identification of material regulatory compliance risks and their corresponding remediation plans
  - Accuracy of reporting on compliance to Senior Management and the Board or Committee(s) of the Board;
  - Assessment of how effectively the Compliance oversight function fulfills its responsibilities.
- Review findings and recommendations that are considered significant should be reported, as appropriate, to operational management, the CCO, Senior Management and the Board.

7. Adequate Documentation

- Produce sufficient documentation for both day-to-day and independent oversight review levels of key control elements that demonstrates how regulatory compliance risk is managed.
- Should preserve the flow of information reported to the CCO, Senior Management and the Board, and be used in the Board's periodic assessment of the RCM framework.

I. OSFI Guideline E-13: Insights into Key Elements

8. Role of Senior Management

- Implement the RCM framework that has been reviewed and discussed with the Board.
- Ensure that:
  - RCM framework is designed, implemented and maintained in a manner that is tailored to the needs of each business activity
  - Compliance policies and procedures are adequate and appropriate to control regulatory compliance risk and applied according to their terms by qualified individuals
  - Key results of day-to-day compliance controls and independent oversight functions are reported to those who need to know
  - Compliance policies, procedures and practices are regularly reviewed to ensure they remain applicable in light of changing circumstances and regulatory compliance risk;
  - Findings and recommendations made by the CCO or Internal Audit or other independent review function are acted on in a timely manner
  - All staff understand their responsibilities for complying with such policies, procedures and processes, and is held to account.

I. OSFI Guideline E-13: Insights into Key Elements

8. Role of Senior Management (Continued)

- Proactively consider whether RCM deficiencies identified in one area of the FRFI's operations may also be present in other areas.
- With regards to the Compliance oversight function, ensure that Compliance:
  - Has the appropriate resources and support to fulfill its duties
  - Is sufficiently independent of operational management
  - Has the capacity to offer objective opinions and advice to Senior Management and the Board.

I. OSFI Guideline E-13: Insights into Key Elements

9. Role of the Board of Directors

- Holds ultimate responsibility for effective enterprise-wide regulatory compliance management.
- Review and understand:
  - Remedial actions taken with respect to instances of material non-compliance or control weakness
  - The FRFI's exposure to material regulatory compliance risk
  - Significant RCM policies
  - The RCM framework and its overall effectiveness.
- Approve:
  - The mandate, resources and budget for the Compliance oversight function
  - Where appropriate, the appointment, performance review and compensation or the COO.

I. OSFI Guideline E-13: Insights into Key Elements

9. Role of the Board of Directors (Continued)

- On a regular basis:
  - Review and discuss findings and reports of the Compliance oversight function
  - Monitor progress in implementing remedial measures for material problems or issues
  - Reassess the effectiveness of the Compliance oversight function and RCM framework
  - Direct and follow-up on improvements in these areas, as necessary.
- Think critically about and challenge CCO reports and Internal Audit or other independent review function reports.
- Satisfy itself that it receives the information required to perform its RCM oversight responsibilities, including seeking assurances from Senior Management that the RCM controls have been implemented and are effective.

II. Regulatory Compliance Management (RCM) versus Legislative Compliance Management (LCM)

- According to OSFI's Guideline Impact Analysis Statement, the main objectives of the revised Guideline E-13 are to:
  - Outline expectations with respect to control frameworks for mitigating regulatory risk
  - Promote industry best practices in regulatory compliance risk management
  - Be more consistent with OSFI's Supervisory Framework (2010) and Corporate Governance Guideline (2013)
  - Be more consistent with international risk management standards.
- By revising Guideline E-13, OSFI has provided more guidance to FRFIs on key control elements.
- Full implementation of the revised Guideline is expected no later than May 2015.

III. Potential RCM Issues seen in practice

Following are illustrative common potential RCM issues seen at Fis. For consideration in general audit scoping:

1. Inventory of Regulatory Requirements does not cover the full breadth of governing legislation and regulations. The Inventory may be focused only on traditional financial services regulations (e.g. Insurance Act, OSFI Guidelines, AML).
2. There is not a comprehensive and robust risk assessment methodology that has been designed and applied against the Inventory of Regulatory Requirements. This can result in inaccurate risk ratings creating regulatory risk and cause the FRFI to misallocate resources and design and implement controls over low or medium risk areas.
3. No clear and complete mapping of regulatory requirements to the business units and to the business processes and controls.
4. Insufficient testing of the design and operating effectiveness of the regulatory controls by the business unit. Insufficient Compliance monitoring and/or independent testing over the controls within the business units.
5. Inadequate regulatory related monitoring and oversight controls over third party service providers. Controls are usually substantially operationally focused, with little to no consideration for regulatory compliance related issues and status at the vendor.

III. Potential RCM Issues seen in practice

6. Comprehensive regulatory issues management process is not in place to allow timely root cause analysis to meet business, customer and regulatory expectations. This increases the likelihood that associated regulatory risks may go unresolved and/or not be fixed in a timely manner.

7. Insufficient training coverage for high risk regulatory requirements. Generic, overarching training provided; however, specific regulatory training is not fully delivered. Insufficient review and controls to ensure that third party service providers are also adequately trained on regulatory matters pertaining to the FRFI's outsourcing activities.

8. Detailed compliance reporting based on a narrative format used within the FRFI. There is limited use of dashboards, key indicators, and a broad forward looking perspective to help focus the RCM framework status and material compliance issues for the Board and Senior Management review.

9. Mandates and position job descriptions are not robust regarding RCM responsibilities. Rather there are generic high-level statements requiring the position holder to maintain a good working knowledge of the laws and regulations applicable to the FRFI.

10. Regulatory compliance is not embedded into business as usual operations. Regulatory compliance is seen as additive to the business units. This scenario can result in increased regulatory risk.

11. Comprehensive technology solution not in place and integrated with the business unit and Compliance RCM processes.

IV. Conclusion

- OSFI considers effective regulatory compliance management essential to a FRFI's well-being. Accordingly, an effective RCM framework is necessary to ensure the FRFI is in compliance with applicable regulatory requirements.
- To help FRFI's establish effective RCM frameworks, OSFI has issued a revised E-13 Guideline to better align with international risk management standards and similar OSFI publications, promote industry best practices, and provide greater detail surrounding regulator expectations.
- Guideline E-13 details key control elements, including day-to-day controls as well as independent oversight, and specific expectations surrounding the roles and responsibilities of various individuals involved in the assessment and management of regulatory risk.

Other Presentations

The other presentations that were presented as part of the Risk and Regulatory series are:

- IFRS 9 Classification, Measurement and Impairment (Insurance Sector): Initial Considerations
- The New World of Cyber Resiliency
- Market Conduct
- ORSA – Next Steps

Presenters

Mary Trussell
Partner
Audit Services
T: +1 647-777-5428
E: mtrussell@kpmg.ca

David Pelkola
Director
Financial Risk Management
T: +1 416-777-8761
E: dpelkola@kpmg.ca

cutting through complexity