Deloitte.

How IA function provides assurance on managing conduct risk
BFIIA Webinar

23 November 2022

Speaker Profile

Richard Chung Cher Shen
Director, Risk Advisory
Deloitte Singapore
cherchung@deloitte.com
+65 6800 2335

Qualifications & professional affiliations

- Chartered Accountant (Singapore)
- Certified information Systems Auditor and CRISC
- Accredited Business Continuity Planner and Expert
- Certified Internal Auditor

Cher Shen has over 16 years from both the commercial and professional sector and is leading the Risk Management, Data Privacy, Governance & Compliance, Internal Controls review, Business Continuity Management and Business Process Re-engineering service lines. He was a former Risk Manager for Singapore Telecommunications. He was a key author of a Singapore Institute of Director Corporate Governance Guides on its Board Risk Committee Guidebook. The guidebook is used by leading risk practitioners as a benchmark in Risk Management implementation for listed Companies in Singapore.

He is also a regular speaker at various external and internal training seminars covering risk management, internal controls and processes best practices.

Prior to joining the firm, he was the Head of Department and a Vice President of Enterprise Risk Management function in a major food conglomerate Company.

He was credited with the successful implementation of risk analytics as part of the Company's risk sensing capability for its ERM programme. The work included obtaining supply chain intelligence from relevant industrial databases (e.g. World Health Organisation) to perform possible risk impact and disruptions studies to the organisation's supply chain before any impact to the organisation could happen.

Nassaya Sitthichokvarodom
Senior Manager, Risk Advisory
Deloitte Thailand
nsitthichokvarodom@deloitte.com
+66 (0) 2 034 0000 Ext. 14037

Qualifications & professional affiliations

- Anti-Money Laundering Experts Certificate (CAM), AMLO
- Governance Risk Compliance Professional (GRCP), OCEG
- Certified Data Privacy Solution Engineer (CDPSE), ISACA

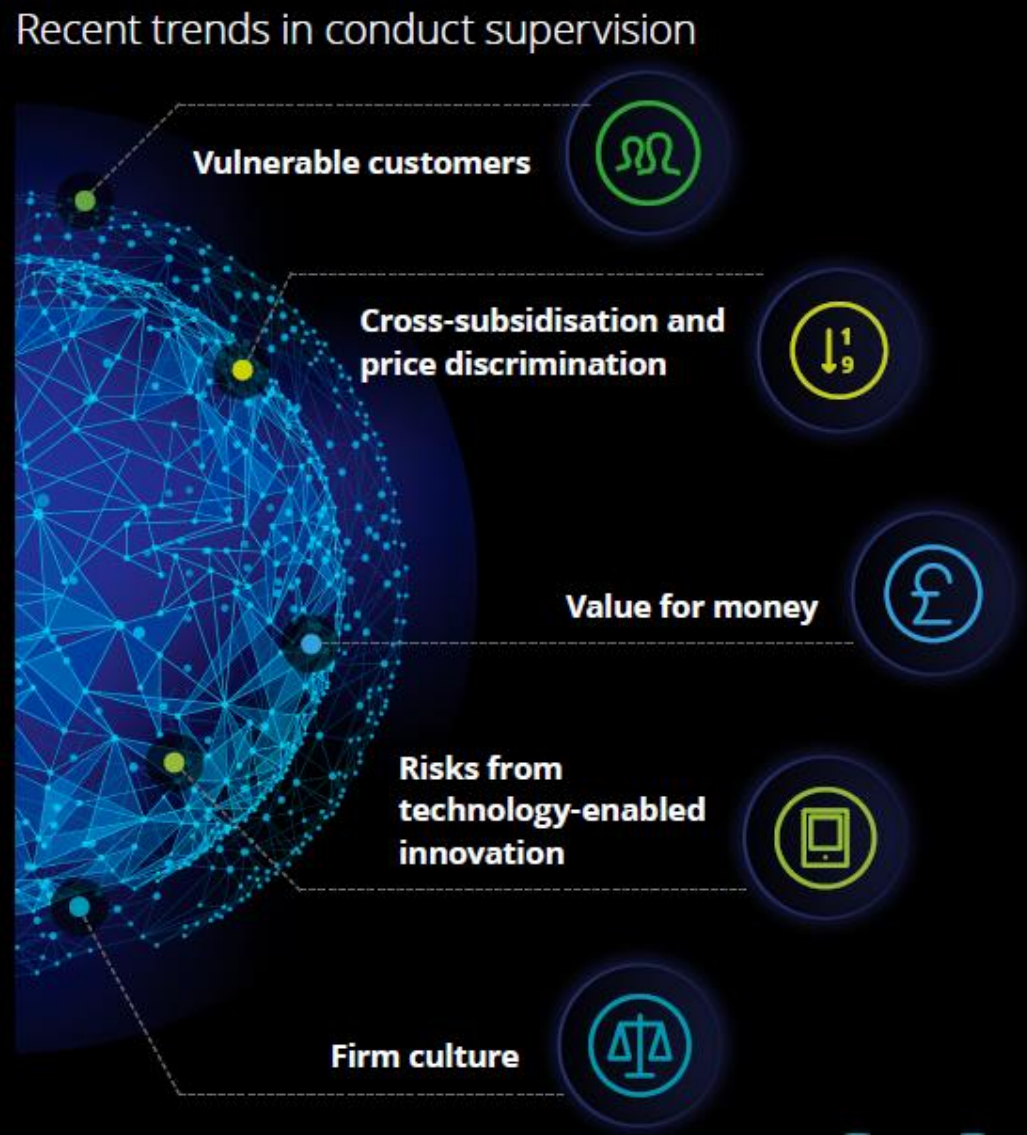
Nassaya is a senior manager in Risk Advisory. She has 12 years of professional experience in consulting services. Nassaya has advised on internal control process of financial institutions covering banking operation, operation of securities company, operation of insurance company.
In addition, She has expertised in enterprise risk management and governance, risk and compliance (GRC) framework for financial institutions and manufacturing companies. The experiences have covered the framework and policy formulation and procedure or process improvement including services of gap assessment against the local regulatory requirement or international standards and providing the robust recommendations.

Experienced Engagements:

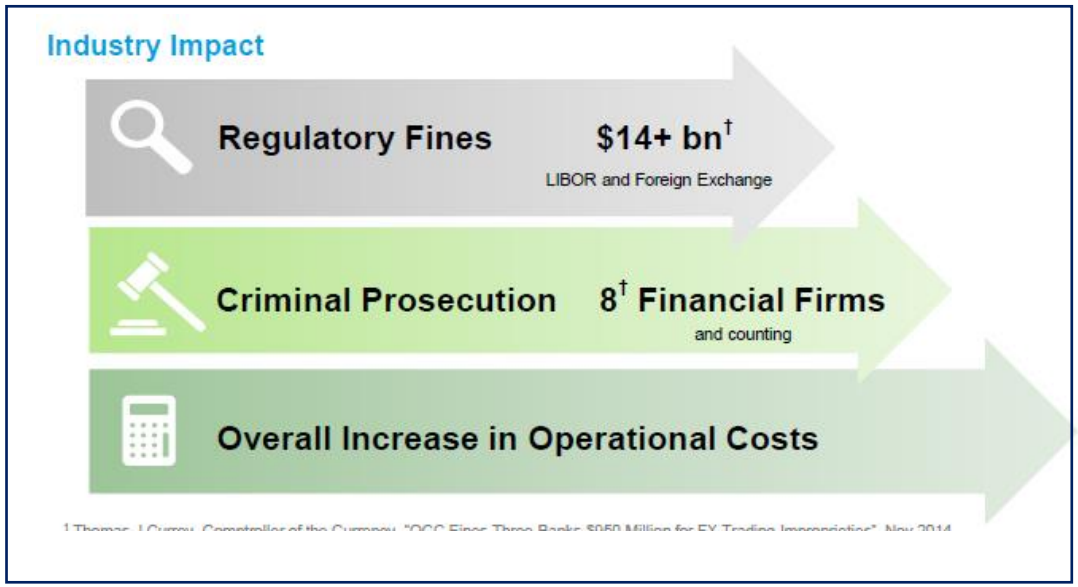
- Enterprise Risk Management (ERM) and Governance, Risk, and Compliance (GRC) Advisory covering end-to-end process (advisory and solution)
- Risk Culture Model Advisory
- Risk Management Mechanism Advisory covering end-to-end process and all level, especial significant risk management in FSI
- Internal Control Review and Audit Services

Deloitte.

Contents



Industry Impact



Enforcement Actions Media Releases | Published Date: 31 August 2022

MAS Imposes Composition Penalty of $375,000 on UOB Kay Hian Private Limited for business conduct and AML/CFT failures

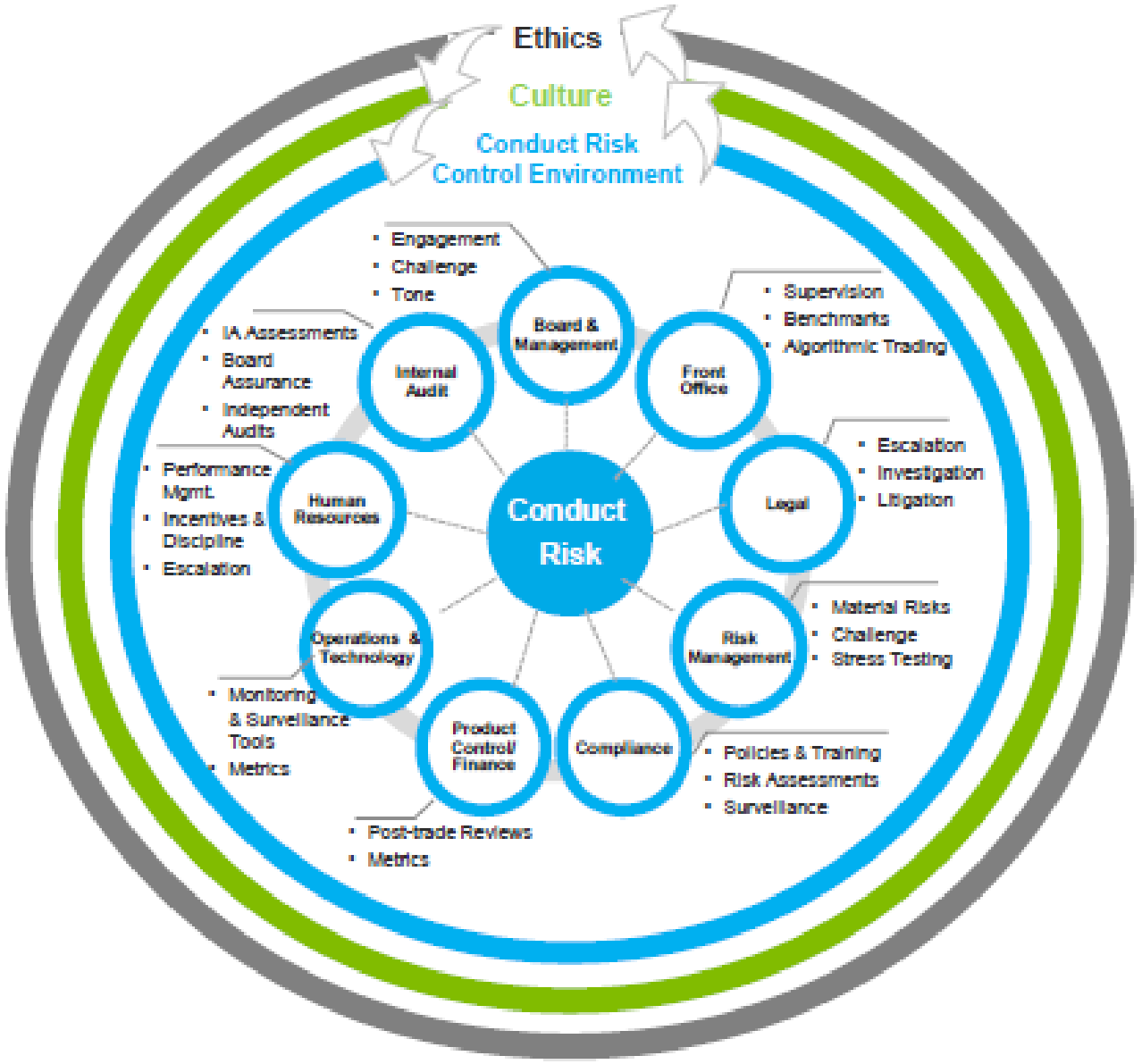
Singapore, 31 August 2022… The Monetary Authority of Singapore (MAS) has imposed a composition penalty of $375,000 on UOB Kay Hian Private Limited (UOBKH) for its failures to comply with business conduct requirements under the Securities and Futures (Licensing and Conduct of Business) Regulations (SFR) and anti-money laundering and countering the financing of terrorism (AML/CFT) requirements under MAS Notice SFA04-N02. These failures were identified during an inspection by MAS. UOBKH has paid the penalty in full.

- There are numerous instances of poor business practices within the financial services industry that have been exposed across the globe have resulted in clients' interests being disregarded, unfair, and inequitable outcomes, considerable financial impact for customers, and damage to the integrity of the market.

- Institutions are facing enhanced regulation, hefty penalties, and substantial remediation costs as a result. Instances of inappropriate behaviour by employees have led to 'conduct costs' in fines, legal bills, and customer compensation of US$14 billion (~THB $500 billion) at the 8 banks in recent years.

- The Bank of Thailand is escalating the punishment for banks that violate the regulator's market conduct rules. Institutions that fail to conform to the central bank's guidelines will be subject to fines up to (THB $1 million) per day, among other penalties.

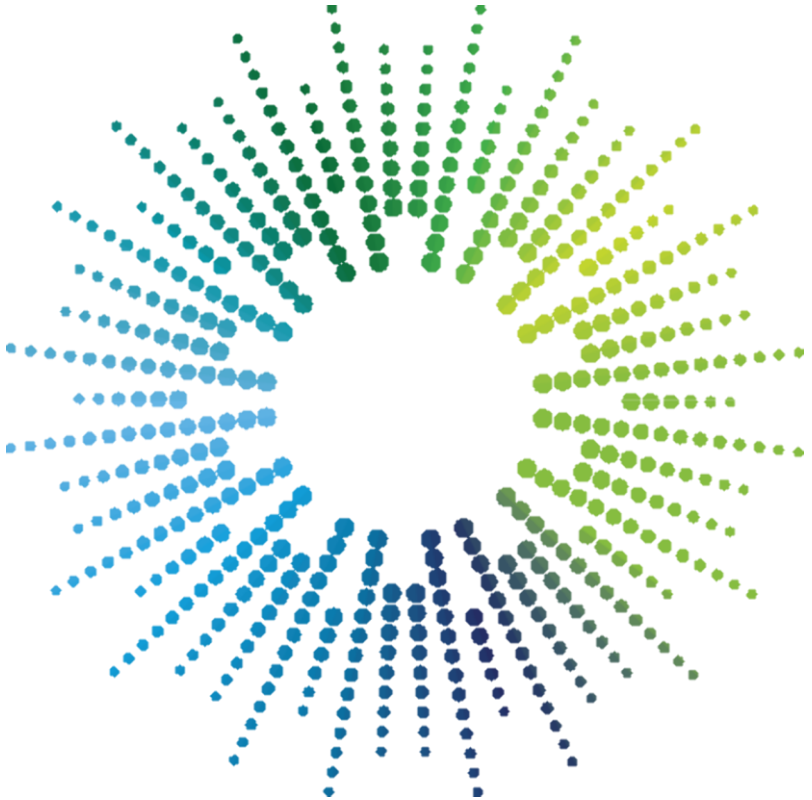
Methodology



Conduct Analytics

- Robotics automation can limit the possibility of conduct risk by reducing the number of manual activities and making routine procedures more consistent. Beyond this, cognitive technologies and data analytics can analyse employee communications, such as emails and text messages, to identify patterns of behaviour that may be inappropriate and warrant additional investigation.

- We believe that banks can leverage advanced analytics to adopt a more proactive approach to managing potential employee misconduct by:
  - Identifying and monitoring leading indicators of potential poor behavior.
  - Developing conduct risk profiles at the individual or sub-group levels which correlate the multiple data points.



Employee Conduct – Core Metrics

Conduct Metric	Analytics	Insights derived
Periodic mandatory training non-completions	➢ Number of non-completions and number of days late by individual over a period (with false positives removed eg: non-completion when someone is on maternity leave/ long term sick leave/ career break) ➢ Records of intervention by line managers (evidence of chasing, number of additional reminders)	➢ This could indicate either a lack of understanding of or disregard for the policy/ deadlines and compliance.
Number of whistleblowing incidents (through different channels eg: anonymous calls. mailbox)	➢ Difference between number reported and number upheld. ➢ Trend analysis over time	➢ High numbers could indicate a culture of feeling comfortable to speak up and/or that multiple behaviours need to be addressed. ➢ Conversely, low numbers could indicate a culture that suppresses reporting or a retaliation culture.
Breaches of gifts and entertainment thresholds	➢ Breaches by individual and by Business Unit / level of seniority. ➢ Trends over time in numbers and materiality of breaches	➢ Potential evidence of conflicts of Interests that may not have been disclosed could be predictive of a lack of transparency, a culture of disclosure or other misconduct eg: sharing of price-sensitive information.

Employee Conduct – Core Metrics (continued)

Conduct Metric	Analytics	Insights derived
Periodic written employee appraisals/ performance management/ 360 feedback	➢ Reconciliation of rating received with qualitative information ➢ Comparisons across Business Units ➢ Trend analysis over time by individual	➢ Multiple mismatches or inconsistencies between rating and qualitative information could be indicative of lack of honesty in feedback provision, inconsistent application of the Conduct Framework, a lack of application of a balanced scorecard approach and/or a failure to reward good conduct and deal with misconduct effectively.
Breaches of mandatory block leave (e.g. did not take the required block leave or broke the block leave policy by logging on and the activity conducted while logged on)	➢ Trends in breaches over time by individual/ Business Unit ➢ Severity of breach and joining the dots with whether any Market Conduct issues were also logged during the block leave period ➢ Cohort analysis across Business Units	➢ Potential joining of the dots with Market Conduct breaches e.g. if a breach of block leave involved any unauthorized trading activity there may be a need for additional focus on specific individuals. ➢ Cohort analysis may reveal wider cultural issues within the department / level of seniority.
Breaches through non-declaration of Personal Account Dealing and Outside Business Interests	➢ Trends in breaches over time by individual ➢ Cohort analysis across Business Units	➢ Potential joining of dots with other data such as websites visited, out of hours trading could be indicative of misconduct intentions and, if reviewed in a timely manner, may support predictive analytics on misconduct.

Market Conduct – Core Metrics

Conduct Metric	Analytics	Insights derived
Time-stamping for sequencing of orders (instances where orders have not been executed in the sequence in which they were received e.g. internal orders have been prioritised over external orders)	➢ Daily comparisons [time] ➢ Hotspots within Business Units	➢ Evidence of policy breaches requiring action and remediation prior to client complaints.
Number and sizes of pricing discounts offered to clients outside of specified range (and associated documentation / sign-off by Business Unit and by individual of any pricing discounts provided and rationale)	➢ Hotspots within particular Business Units/ individuals/ geographies / levels of seniority ➢ Trends over time relating to individual traders	➢ Any instances of favoritism of one client leading to unfavorable outcomes for other clients, which could be identified and remediated prior to customer complaints and lead to further controls being developed.
Instances of price-sensitive information being shared (e.g. inside information)	➢ Sampling and key words identified through surveillance to highlight instances of market abuse ➢ Periods where breaches are more common ➢ Hotspots within particular Business Units/ individuals/ geographies / levels of seniority ➢ Cross-referencing with data leakage incidents	➢ Sharing of price-sensitive information could highlight broader misconduct issues among individuals and could be indicative of supervisors not providing sufficient oversight.
Risk/reward/behaviour balance on new products and exceptional deals	➢ Balanced scorecard usage over time ➢ Outliers compared to average risk/reward balance	➢ Understanding of reward in the context of how profit was generated - the balanced scorecard approach should mean reward is dependent on the amount generated in profit as well as how this is generated (i.e. the conduct/behaviors displayed).

Behavioral Analytics profiles (Group/ Individual)

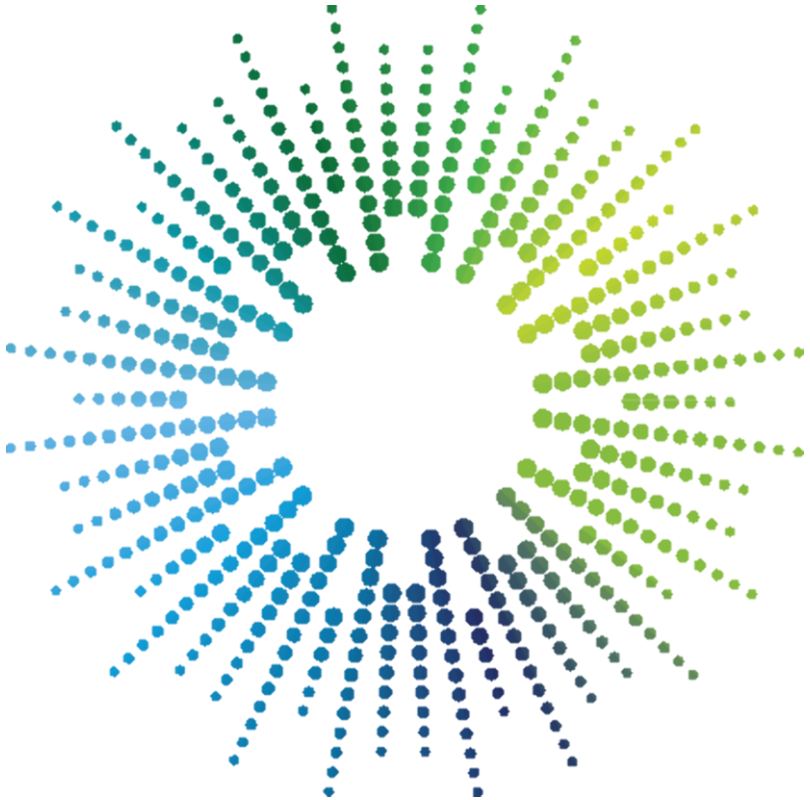
		Employee 1	Employee 2	Employee 3	Employee 4	Employee 5
Behavioral	Training: Non-completion of compliance related trainings per year					
	Personal trading (PT): PT policy violation per year*					
	Limit Breach: Established Market limit breach per year*					
	E-communication warning/flagging received per year					
	Time and expense abuses (i.e., excessive spending)					
	Any other policy violation					
Performance	Fraud					
	Bonus Flux %: Change in bonus year over year					
	Tenure: Time spent in the organization					
	Compensation Deviation: Standard deviation of compensation from 90 percentile of his/her peer group					
	Performance History: Performance status of individual for past 4 years					
	Promotion history or upcoming promotion					
	Performance vs key metrics (e.g. sales targets, productivity)					
Other Internal data	New role due to transfer					
	Behavioral risk attributes					
	Divisional performance and earnings pressure					
	Divisional performance/earnings fluctuation					
	Layoff rumors (social sentiment)					
	Web activity (e.g. sites visited, time on internet etc.)					
External Data	Postings on LinkedIn					
	External economic factors (i.e., recession)					
	Marital status					
	Bankruptcy history					
	Credit score					
	New home purchase					
		Tier 2	Tier 3	Tier 1	Tier 2	Tier 1

Considerations for Data Analytics

Key considerations around reducing sensitivity in analysis are:

- Human intervention around models: When analyzing behaviors signals it is not possible to remove subjectivity entirely, but processes can be designed to try minimize this risk. As it is not possible for monitoring teams to oversee every single event, a system can build the funnel and filter to highlight any potential misconduct or poor conduct issues. Human intervention is then deployed at the point that the system identifies a potential issue.

- Predictive analytics: When applying such analytics to behavioral metrics, there can be conscious or unconscious bias in implementing preventative controls on specific individuals based on an increased likelihood of a misconduct event occurring. Predictive analytics could be used to identify increased risks of misconduct occurring and can be used to triage incidents and rank likelihoods as higher or lower risks. This can then facilitate human checks and requirements for preemptive steps to be taken, such as further investigation in a specific area.



IA Assessment

Types of assessment techniques to assess the conduct risks:

- Governance and Oversight: robust governance structure, defined roles and responsibilities across the business and demonstrated oversight of remedial measures
- Internal Controls and Compliance Program: common conduct risk taxonomy, business led risk assessment, inventory of key business activities, policies/procedures and internal controls, key risk indicators and associated metrics.
- Compliance Risk Management Program: challenge of business risk assessment and Compliance Testing program to assess conduct risk.
- Internal Audit Program: specialized focus area on market conduct risk, including incorporation into audit planning, risk assessment and execution

Board Assurance – Promoting Accountability amongst Senior Managers

Senior Managers responsible for managing and conducting the financial institution's core functions are clearly identified.

- Senior Managers with responsibility for essential functions, including but not limited to core management functions (CMFs), should be identified.
- **Senior Managers identified should reflect actual oversight responsibilities** and decision-making authority, regardless of their physical location.
- The Senior Manager's seniority within the organisation and other relevant circumstances must be taken into consideration during the identification process.
- Senior Managers should in general have direct reporting lines to the CEO or to the Board and Head Office.
- Non-executive board directors would not be considered Senior Managers.

Senior Managers are fit and proper for their roles and **held responsible for the actions of their employees** and the conduct of the business under their purview.

The financial institution's governance framework supports Senior Managers' performance of their roles and responsibilities, with a clear and transparent management structure and reporting relationships.

- Financial institutions should conduct the necessary due diligence prior to appointing Senior Managers.
- Financial institutions should clearly articulate the roles and responsibilities of their Senior Managers in relation to their operations, and their overall management structure.

Board Assurance – Promoting Accountability amongst Senior Managers (continued)

The financial institution's governance framework supports Senior Managers' performance of their roles and responsibilities, with a clear and transparent management structure and reporting relationships (continued).

- Financial institutions should ensure **robust standards and processes** to assess the fitness and propriety of Senior Managers, proper governance, documentation, clear reporting lines, and updated succession plans.
- Financial institutions should establish **an appropriate incentive framework** based on a range of factors, **including non-financial key performance indicators**, risk management, control lapses, or other conduct matters.
- Financial institutions should establish **a formal mandate and articulate the terms of reference and reporting lines for each committee**.

Board Assurance – Strengthening Oversight of Material Risk Personnel

Material risk personnel are fit and proper for their roles, and subject to effective risk governance, and appropriate incentive structures and standards of conduct.

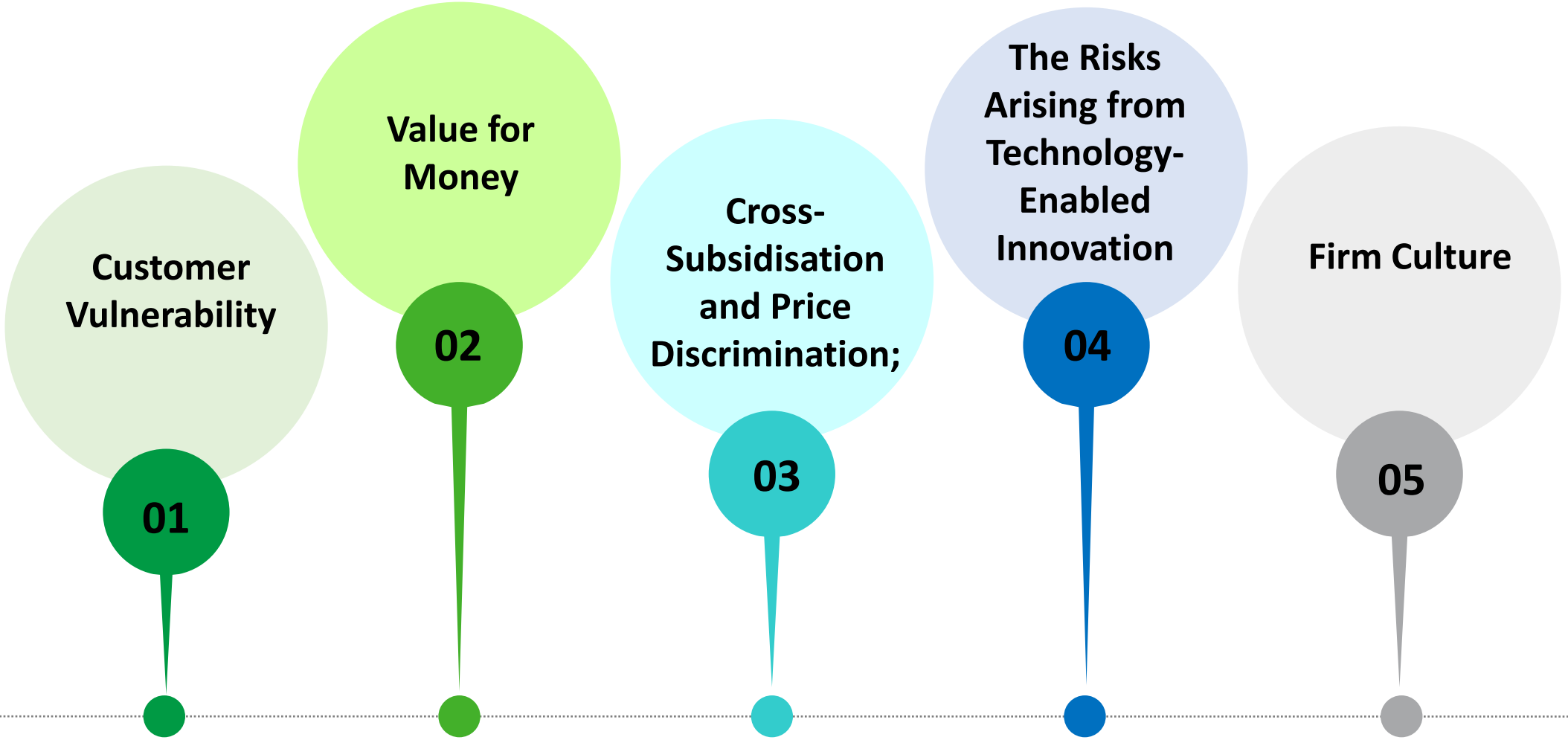
- Financial institutions should identify material risk personnel based on two primary considerations: risks that a financial institution is exposed to due to the nature, size, and complexity of its business; and individuals who have the authority to make decisions or conduct activities that could have material quantitative or qualitative impacts on its risk profile.
- Financial institutions should assess the fitness and propriety of material risk personnel and subject them to standards of proper conduct, regular training, and an appropriate incentive structure.
- The international regulators (e.g. MAS) does not intend to introduce additional registration or notification requirements on material risk personnel, and financial institutions should maintain information on their material risk personnel to facilitate oversight of their activities.

Board Assurance – Promoting Proper Conduct amongst all Employees (continued)

The financial institution has a framework that **promotes and sustains among all employees** the desired conduct.

- **Financial institutions should ensure that a framework is in place** to address the standards of conduct expected of all employees and ensure consistent and effective communication of the standards.
- Financial institutions should establish appropriate policies, systems, and processes to enforce the expected standards of conduct including regular monitoring, reporting, and a consequence management framework.
- **The Board and Senior Management should notify the regulator as soon as** they become aware of any material adverse developments, such as misconduct, lapses in risk management and controls, or breaches in legal or regulatory requirements that have the potential to cause widespread disruption.
- **The regulator should also be notified in a timely manner** of any information that may have a material negative impact on the fitness and propriety of Senior Managers or material risk personnel.
- Financial institutions should put in place the appropriate metrics for monitoring conduct, including both quantitative and qualitative indicators of positive and negative conduct.

Recent Trends in Conduct Supervision



Recent Trends in Conduct Supervision (Cont.)

Customer Vulnerability

- Firms will need to demonstrate what measures they are taking to identify vulnerable customers, both within their existing customer base and on an ongoing basis, bearing in mind that vulnerability is a complex, dynamic state. Once vulnerable customers are identified, supervisors will further expect that these customers have been treated fairly, their needs met and their circumstances kept under review.

Areas of supervisory enquiry:

- The identification of vulnerable consumers.
- The monitoring of existing customers for signs of vulnerability or changes in circumstances which may result in vulnerability.
- The reassessment of vulnerable customers and their circumstances.
- How the firm's products and/or services meet the needs of vulnerable customers.
- The assessment of the potential impact of strategic decisions or known events on vulnerable customers.

Firm Culture

- Culture has become a key focus for supervisors in their strategic response to the global financial crisis and subsequent misconduct scandals. Supervisors will challenge the Board and Senior Managers on how they assure themselves that their target culture is operating in practice and delivering acceptable outcomes, from a regulatory, strategic and commercial perspective.

Areas of supervisory enquiry:

- The extent to which the firm and its employees prioritise good customer outcomes over mitigating risks or commercial benefits.
- The extent to which the firm's culture attaches the right importance to issues such as vulnerable customers, cross-subsidies, etc.
- The values and attitudes of staff and how these are developed.
- The culture and values of the Board and Senior Managers, how these are monitored and the influence they have on the wider firm.
- How the Board and Senior Managers ensure that staff understand conduct risk and its importance to the firm.
- The degree of confidence the Board and Senior Managers have that employees escalate important issues.

Case Study – Sales of higher risk products to vulnerable customers

Background

A Major Australian Bank undertook a targeted review of their product and customer portfolio, to understand if their products aligned to customers' needs and expectations.

Journey

Risk & Lens Workshops

- Exploration and identification of risk factors relevant to customer behaviour
- Generation of hypotheses and risk profiles

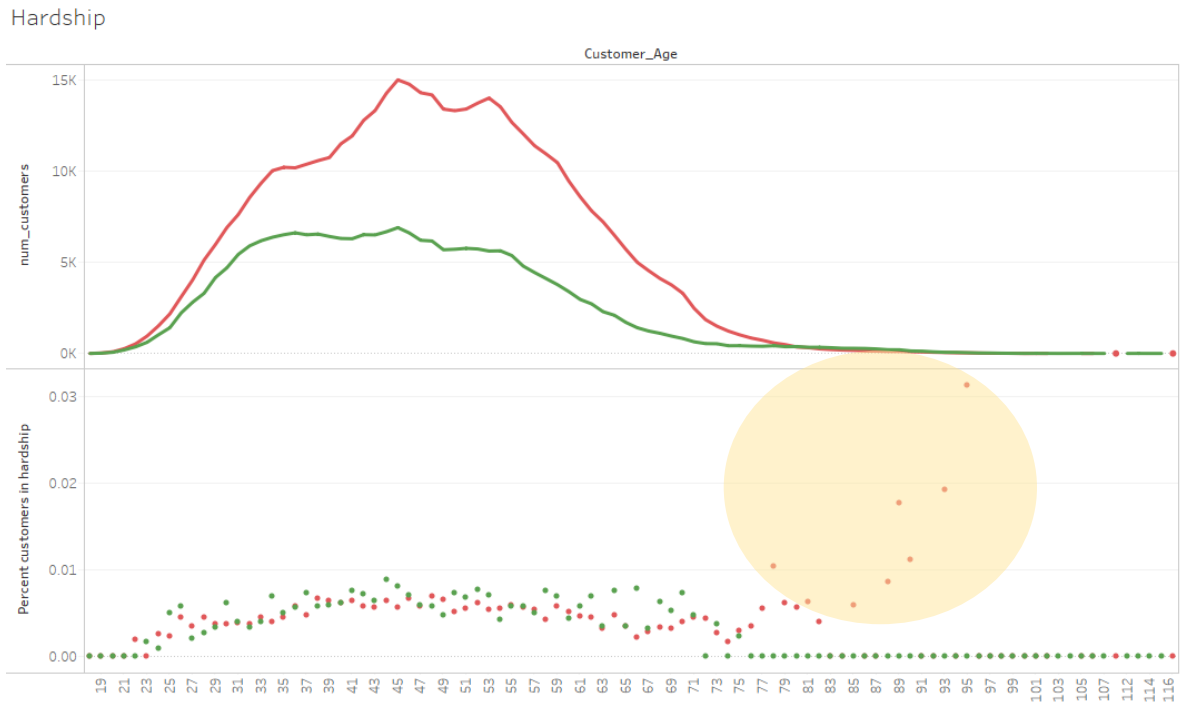
Data Acquisition & Structuring

- Assessment of data landscape
- Extraction, transformation, loading of data
- Determine and agree KRIs and associated metrics for assessing 'outliers'

Analytics

- Analysis of data with the application of coded rule-sets
- Review and observe customer distribution and outliers against thresholders
- Identification of 'at risk' customers and risk drivers

One of the insights discovered was that certain senior customers in a particular brand had a greater likelihood of being in hardship. While the issue was not systemic, proactive outlier reporting was recommended as an action to equip to look forward.

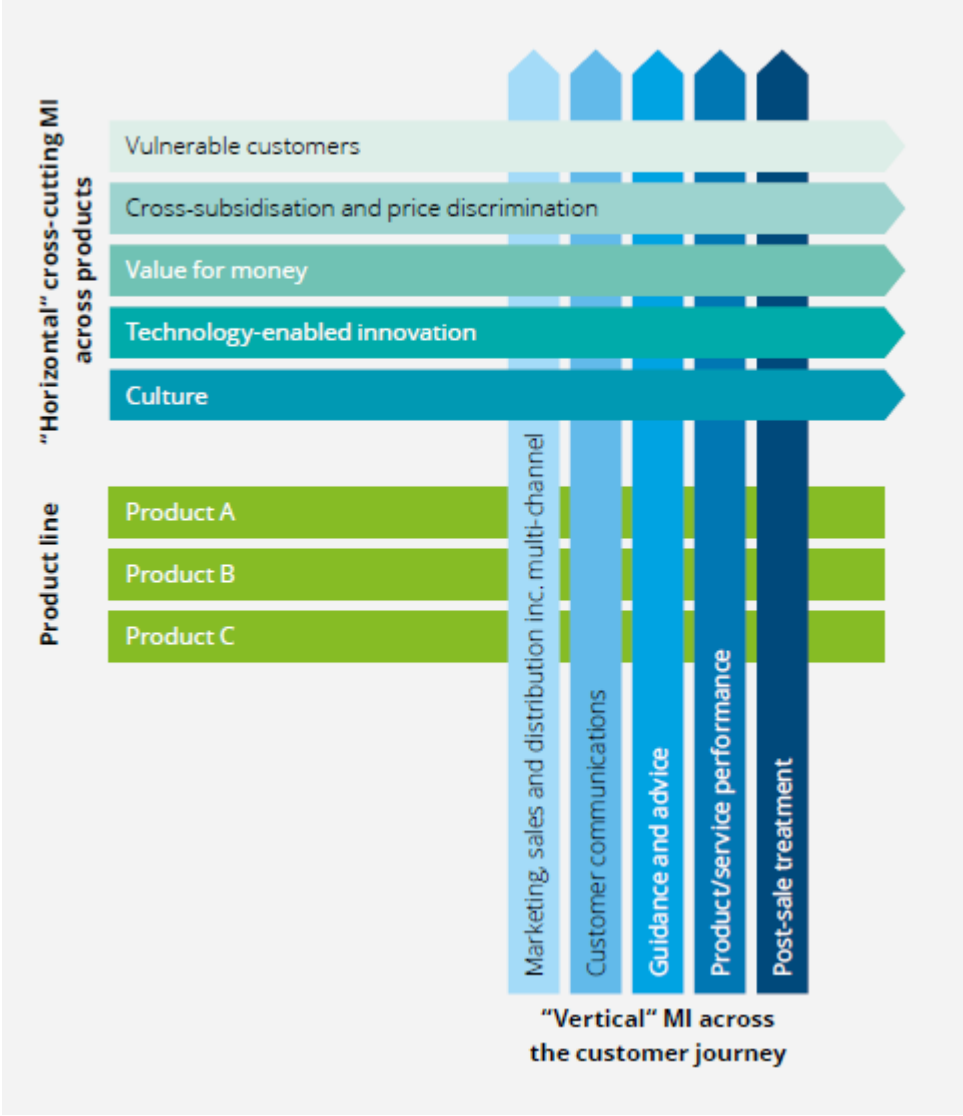


The Importance of Cross-Cutting, Horizontal MI to Proactive Conduct Risk Management

This horizon scanning should pay particular attention to emerging risks and themes (for example, themes highlighted across several jurisdictions or sectors) and high priority issues as well as the lessons learned from wider misconduct scandals and enforcement actions.

Thematic reviews could analyse emerging regulatory trends from a number of different angles to identify whether they give rise to specific risks and issues within the business. Issues around value for money, for example, could be identified:

- across products- assessing whether certain products offer poorer value for money than others;
- across business lines- identifying whether divergent approaches to assessment of value for money in different parts of the business create poor outcomes for some customers;
- across customer segments- determining if certain groups of customers receive poorer value for money than others; and
- across the customer journey- identifying whether a given product continues to offer customers value for money on an on-going basis.

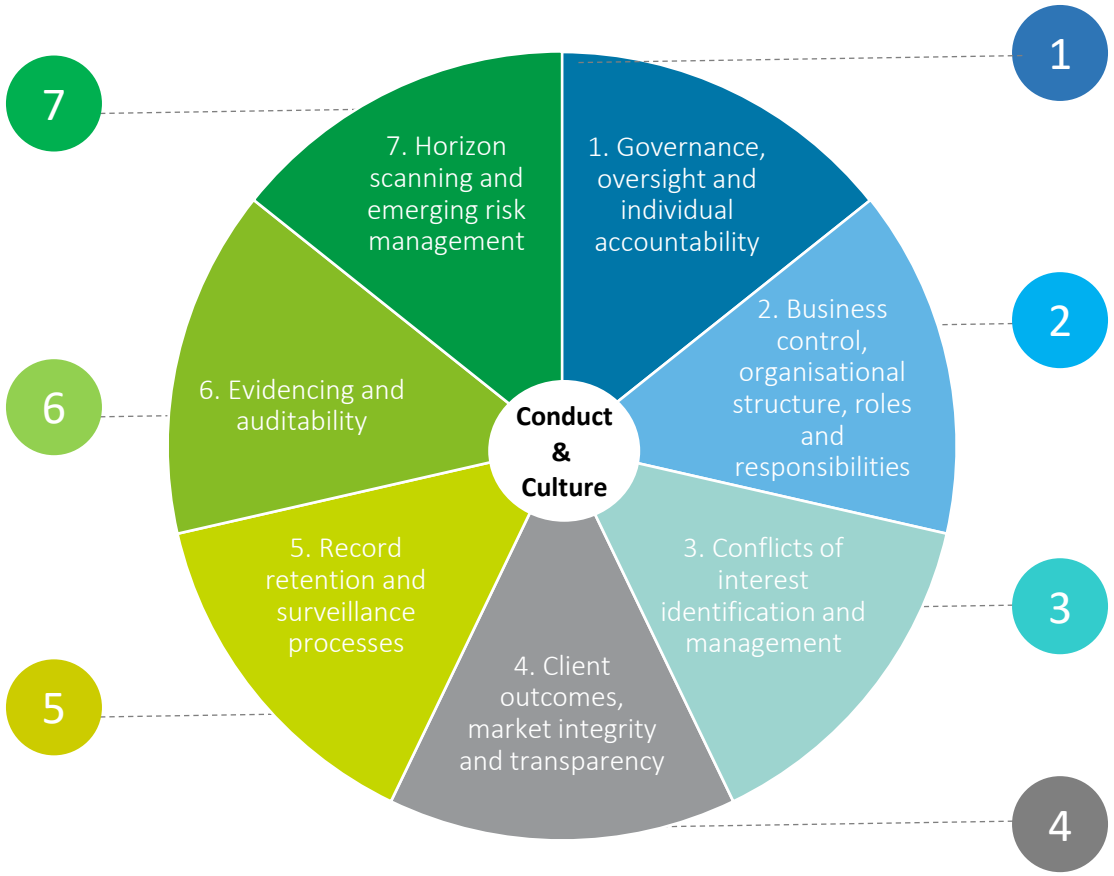


Areas under Increased Regulatory Scrutiny for Conduct Risks

- Focus on actionable and meaningful MI to help identify thematic emerging risks
- Can be used effectively to monitor effectiveness of detective and preventative measures, and fine tune predictive capabilities

- Evidencing challenge of governance and demonstrating reasonable steps
- Rise of enhanced assurance from Audit on management of key conduct risks
- Positive affirmation and review of “risk-based methodologies” for key controls

- Global inconsistencies in period of retention and surveillance capabilities for eComms and Voice
- Continued expectation to retain and retrieve vast volumes of data, quickly
- Requires stakeholder ownership and interaction throughout lines of defense



- Growth of cross functional oversight working groups across the lines of defence
- Use and merit of attestations internally and externally
- Focus on the “tone in the middle”
- Need for effective metrics, KPIs and analytics to demonstrate reasonable steps against misconduct and culture

- Design and implementation control functions
- Collaborative, cross functional control monitoring and reporting (as opposed to silo approach)
- Opportunity to restructure control monitoring across the lines of defense, with the aim of maximizing efficiency and minimizing cost

- Greater focus on the ownership and management of conflicts of interest by the front office
- Embedding into management’s risk and control self-assessments (RCSAs)
- Targeting of consistency in application of conflicts identification and management

- Client perception a key consideration in establishing expectations on acceptable/ethical behaviour
- Greater focus on written guidance on “grey areas” for sales and trading business practices
- Enhanced client disclosures (via disclaimers) and reconfirmation of treatment of orders

How to Design and Strategize a Conduct Risk Management Program?

Firms ***must go beyond a Code of Conduct*** to develop a sustainable conduct risk management program.

Key aspects of a conduct risk management program include...

Essential Components for Addressing Conduct Risk

1. Defining the Conduct Risk strategy

- Summarizing the corporate strategy in terms of growth areas, priorities regarding existing customers, distribution model and organization competencies
- Establishing the risks of misconduct which emanate from the strategy
- Clearly specifying the target outcomes in relation to each conduct risk
- Measures of whether the conduct risk strategy is successful or not are defined

2. Developing the Conduct Risk framework

- Framework that clearly references and appropriately covers the conduct risks faced by the firm (i.e. people, process, system and external events)
- Objectively defining the components of the conduct risk framework across the three lines of defence and structuring a defined communication plan
- Roles and responsibilities in relation to the implementation of and compliance with the framework

3. Developing the Conduct Risk Policy

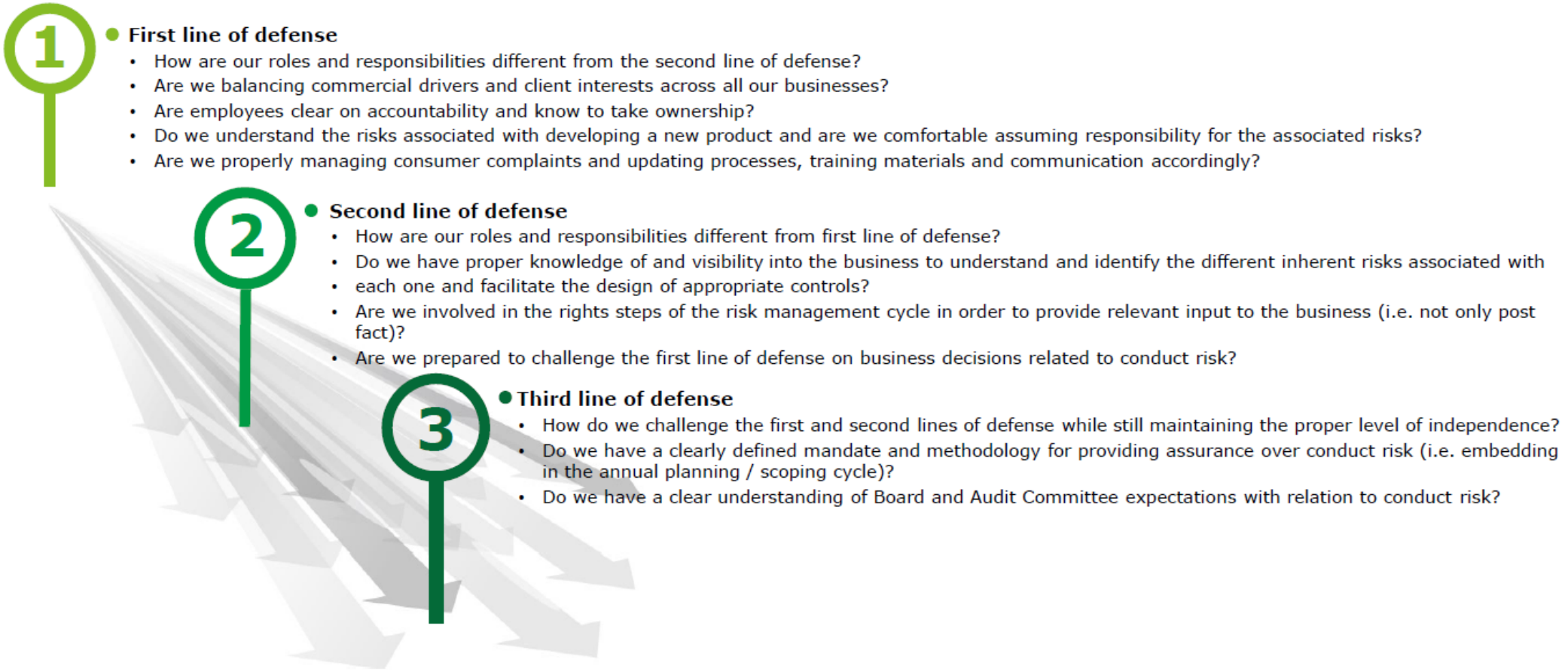
- Comprises: – Firm's conduct risk strategy and objectives – Firm's conduct risk universe across the operating model – Tools and processes for the management of conduct risks – Governance arrangements that are in place for oversight of conduct risk and associated reporting framework – Board mandate in relation of conduct risk

4. Establishing the Conduct Risk appetite

- Conduct risk appetite gives consideration to the whole customer lifecycle
- Each statement is specific enough so that it is not open to misinterpretation
- Takes into account the firm's strategy and key output of the conduct risk framework
- Qualitative and quantitative measures for monitoring performance of the risk appetite

Responsibilities across the Three Lines of Defense

Each of the lines of defense has a role to play in managing conduct risk. How responsibilities are organized and ownership of conduct risk is defined and allocated can vary across the three lines; however, each line should consider the following questions:



First line of defense

- How are our roles and responsibilities different from the second line of defense?
- Are we balancing commercial drivers and client interests across all our businesses?
- Are employees clear on accountability and know to take ownership?
- Do we understand the risks associated with developing a new product and are we comfortable assuming responsibility for the associated risks?
- Are we properly managing consumer complaints and updating processes, training materials and communication accordingly?

Second line of defense

- How are our roles and responsibilities different from first line of defense?
- Do we have proper knowledge of and visibility into the business to understand and identify the different inherent risks associated with
- each one and facilitate the design of appropriate controls?
- Are we involved in the rights steps of the risk management cycle in order to provide relevant input to the business (i.e. not only post fact)?
- Are we prepared to challenge the first line of defense on business decisions related to conduct risk?

Third line of defense

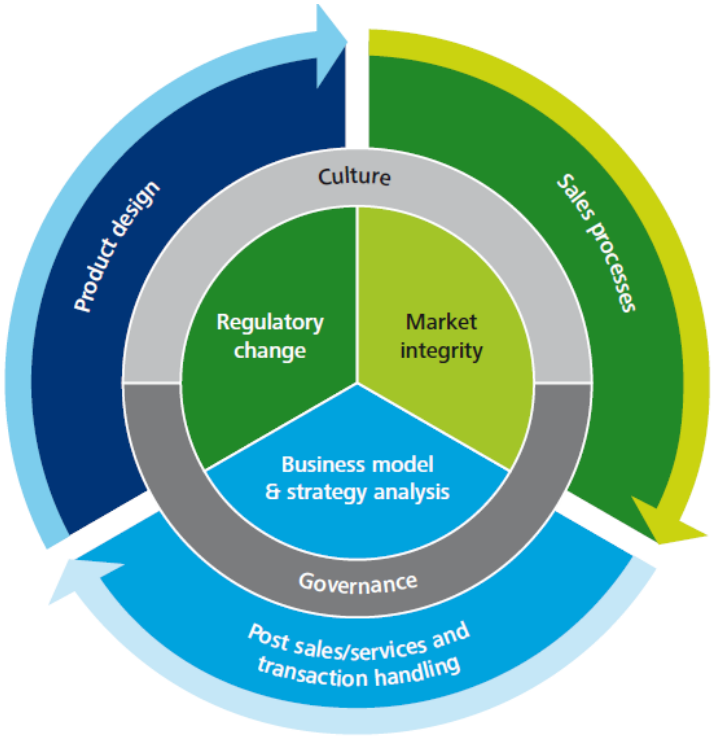
- How do we challenge the first and second lines of defense while still maintaining the proper level of independence?
- Do we have a clearly defined mandate and methodology for providing assurance over conduct risk (i.e. embedding in the annual planning / scoping cycle)?
- Do we have a clear understanding of Board and Audit Committee expectations with relation to conduct risk?

Market trends show the first line increasingly taking ownership over conduct risk, resulting in front office roles such as 'Chief Conduct Officer' or 'Head of culture and Conduct', developing a holistic approach to conduct programs and directly overseeing enforcement of conduct risk management.

Approach to Conduct Risk in Internal Audit

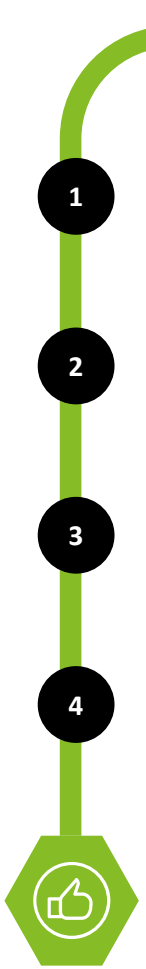
As the focus of the FCA shifts from standalone frameworks to embedded and customer-centric processes, the approach adopted by internal audit should evolve accordingly to reflect this. Conduct risk is not static, nor is it limited to a defined part of the business. It is present in almost every part of the business in different ways, driven by firm strategy, product set and customer journeys adopted by each firm. Consequently, conduct risk will be managed differently within each firm and there is no standard or "off the shelf" approach that internal audit can utilise. Below, we explore four of the drivers which may influence how conduct risk is audited.

1. **Standalone Framework Reviews**
2. **Integration into Existing Activity**
3. **Conduct Focused Reviews**
4. **Competency**



Conduct Risk Key Framework Elements

Is Internal Audit Getting the Right Outcome?



1. **Can you identify the Bank's conduct vision, strategic customer outcomes and key conduct risks?**
2. **Is your Bank saying conduct, or doing conduct?**
3. **What does conduct say about the wider implementation of your three lines of defense?**
4. **Can your internal audit team keep pace with the evolving and expanding conduct agenda?**

Richard Chung Cher Shen
Director, Risk Advisory (Based Singapore)
Tel: +65 6800 2335
cherchung@deloitte.com

Nassaya Sitthichokvarodom
Senior Manager, Risk Advisory (Based Thailand)
Tel: +66 (0) 2 034 0000 Ext. 14037
nsitthichokvarodom@deloitte.com

Deloitte.

Deloitte.

Deloitte Touche Tohmatsu Jaiyos Advisory Co.,Ltd.
AIA Sathorn Tower, 23rd – 27th Floor.
11/1 South Sathorn Road
Yannawa, Sathorn
Bangkok 10120, Thailand

Tel: +66 (0) 2 034 0000
www.deloitte.com

Deloitte.