



# Operational Risk Management (ORM)



# *Business Drivers & Client Questions*

- *What are regulator expectations pertaining to operational risk management? What does that look like in day-to-day business?*
- *How does your operational risk maturity compare to our peers?*
- *How do organizations deploy the three Lines of Defense risk management model without creating duplicative or redundant work?*
- *How can you encourage your front line unit resources to take more ownership of risk? How do you clarify the responsibilities of the 1st vs. 2nd Lines of Defense?*
- *What can be done to encourage the desired risk culture and risk management behaviors?*
- *How can your organization deploy the Enterprise Risk Appetite Statement at the business level?*
- *What risk and control metrics do you need to be monitoring and how frequently?*
- *What tools or processes can be deployed to further automate risk reporting and make it more conclusion based and actionable?*
- *What can be done to help minimize unexpected operational losses?*

# ORM Framework

KPMG has developed a wide-ranging Operational Risk Management Framework that is scalable to individual needs, assists clients with addressing increased regulatory expectations, and strengthens existing risk infrastructure.

## ORM Framework










# ORM Framework Elements

The Operational Risk Management Framework is comprised of seven critical elements and seeks to address regulatory expectations by leveraging applicable KPMG methodologies related to enterprise risk management. A high level description of these key elements can be found below.










# Operational Risk Framework Maturity Model

Operational Risk Frameworks will vary based on a firm's size, complexity and regulatory categorization. The following provides a high level overview of how operational risk components evolve as firms mature and address emerging regulatory expectations.

	Newly Established	Evolving	Mature
 <b>Risk Strategy &amp; Risk Appetite</b>	Strategy and risk appetite defined in silos, regulatory ORM capital only	Strategy and risk appetite defined in tandem, economic ORM capital calculated at enterprise level, allocated to business level	Strategy and risk appetite defined in tandem and cascade to the business level level, economic capital incorporated into product pricing
 <b>Risk Governance</b>	Ad hoc discussions in risk management forums with no business representatives, basic ORM policies in place	ORM committee established (with business partners), ORM Framework established, program specific policies in place, three lines of defense defined	Business owned risk teams, credible challenge mechanisms, roles and responsibilities well defined /accepted, BOD informed of risk taking
 <b>Risk Culture</b>	"Risk management deals with risk", incentives based on growth goals	"Risk is a necessary evil", ORM is a discussion topic in performance management, reactive ORM training after loss events	"Everyone plays a role in risk management", incentive plans linked to losses, reputation, customer impacts, etc. preemptive risk training programs
 <b>Operational Risk Assessment &amp; Measurement</b>	Qualitative enterprise assessments	Qualitative and quantitative enterprise assessments, informal scenario analysis (not linked to Basel categories)	Qualitative and quantitative business assessments, scenario analysis informs capital modeling, internal/external loss data considered
 <b>Operational Risk Management &amp; Monitoring</b>	ORM programs in silos, incomplete coverage, monitoring performed solely by ORM	Full internal coverage, linkages between ORM programs, monitoring performed by ORM and Business	Integrated data / correlated to generate "risk intelligence" that supports decision making / strategic planning, identify ORM trends/thematic events
 <b>Operational Risk Reporting &amp; Insights</b>	Report card on status of ORM program or qualitative reporting capabilities	Enterprise reporting including Key Risk Indicators (KRIs) and tolerances	Consistent reporting structure, across businesses, business level KRIs and tolerances, defined escalation/breach protocols
 <b>Operational Data &amp; Technology</b>	Operational programs/reporting heavily manual	Some automation, but disparate risk data centers/owners	GRC platforms, automated operational programs/reporting with high confidence in data

# Key Components of the ORM Framework Elements

Operational risk elements previously defined have been detailed into key components. These key components link to recent regulatory guidance on minimal standards for enhanced risk management and advanced measurement approaches. A strong, mature operational risk program will likely address all of the components highlighted below.

 <b>Risk Strategy &amp; Risk Appetite</b>	 <b>Risk Governance</b>	 <b>Risk Culture</b>	 <b>Operational Risk Assessment &amp; Measurement</b>	 <b>Operational Risk Management &amp; Monitoring</b>	 <b>Operational Risk Reporting &amp; Insights</b>	 <b>Operational Data &amp; Technology</b>
Strategy & Risk Appetite	Board Oversight and Interaction	Risk Culture	Taxonomy	Testing	KRIs & Risk Limits	IT Architecture and Management
	Committee Organization	Compensation and Performance Mgmt.	Loss Data Assessments	Validation	Mgmt. Reporting and Escalation	Data Governance and Ownership
	Risk Governance Framework	Talent Management Processes	Qualitative Assessments	Risk Mitigation Planning	External Reporting	Risk Data Aggregation
	Roles and Responsibilities	Communication and Education	Risk Control Self Assessment	Incident/Issue Management		System/Tool Selection
	Credible Challenge		Capital Modelling	Customer Complaint Management		Disaster Recovery
	Model Governance and Risk Management		Root Cause Analysis	Change Control and Change Management		Information Security
	Policy and Procedure Management		Scenario Analysis	Third Party and Vendor Management		Technology Enablement
			Loss Collection Criteria	Business Continuity		Near Miss Data

# ORM Framework Component Description

Element	Component	Component Description
Risk Strategy & Appetite	<b>Strategy and Risk Appetite</b>	An organization's approach to achieve its business objectives and its attitude and approach to accepting and managing operational risk. Defines how an organization can achieve its business objectives within the bounds of sound governance and risk management requirements.

# ORM Framework Component Description



Element	Component	Component Description
Risk Governance	<b>Board Oversight and Interaction</b>	Clarified responsibilities, defined accountabilities, and interaction chains for the Board and Senior Management. Provides visibility into an organization's risk profile and business operations to drive effective risk oversight while complying with regulatory requirements.
	<b>Committee Organization</b>	Defined escalation and reporting path structure to fulfill governance and oversight of risk areas.
	<b>Risk Governance Framework</b>	The organization's Operational Risk Framework, commensurate with size and risk profile of an organization, outlining the various components of risk management and how Operational Risk Management responsibilities are fulfilled.
	<b>Roles and Responsibilities</b>	Defined ownership and accountability of the three Lines of Defense, including business leadership, independent corporate operational risk and internal audit, charged with identification, measurement and monitoring of risk.
	<b>Credible Challenge</b>	Feedback loop facilitating independent challenge by second and third Lines of Defense of business risk decisions and activities to drive consistency in risk assessments across the first Line of Defense.
	<b>Model Governance and Risk Management</b>	Robust model governance structure which encompasses model development, model review and model usage standards.
	<b>Policy and Procedure Management</b>	Documentation guiding risk management behaviors and outlining the approach to identify, measure, monitor and control operational risks, including activities and guidelines put in place to develop standardized policies and procedures.



# ORM Framework Component Description



Element	Component	Component Description
Risk Culture	<b>Risk Culture</b>	Common understanding and values embedded through all levels of the organization which support and provide appropriate standards and incentives to drive behaviors.
	<b>Compensation and Performance Management</b>	Compensation, incentive and promotion policies which align to the Operational Risk appetite, establish and reinforce desired risk culture, and balance revenue growth with expected risk management results.
	<b>Talent Management Processes</b>	Resources have appropriate knowledge, skills and training to fulfill risk management responsibilities, and are deployed appropriately to meet the organization's risk management and strategic objectives.
	<b>Communication and Education</b>	Belief and commitment to continuous improvement to enhance management of risk. Open dialogue yielding enhanced comfort, raising concerns and questioning status quo.

# ORM Framework Component Description



Element	Component	Component Description
Operational Risk Assessment & Measurement	<b>Taxonomy</b>	Consistent definition and common architecture for risk terminology and organization allowing for enhanced consistency in data aggregation and reporting.
	<b>Loss Data Assessments</b>	Analysis of incurred and historical operational loss data to align capital allocation requirements.
	<b>Qualitative Assessments</b>	Operational Risk assessment processes which rely on management expertise to evaluate likelihood and severity of risks.
	<b>Risk Control Self Assessment</b>	Creation of risk assessment governance, training, roles and policy to embed risk assessment throughout the enterprise. Identification of risks and evaluation of controls using granular rating methodology.
	<b>Capital Modeling</b>	Aids in more accurate capital allocation methodologies and effective link with risk appetite framework, improving enterprise-wide understanding of risk. Quantitative measurement of a firm's risk profile/capital based on empirical data, expert opinion or both.
	<b>Root Cause Analysis</b>	Analysis of incurred losses to identify process or control failure which led to the loss event and may necessitate changes or enhancements to existing control processes.
	<b>Scenario Analysis</b>	Level of challenge, bias and documentation. Methodology to review data sourcing approach and assess theoretical soundness of model methodology underlying assumptions and algorithms used. Test model implementation accuracy, model sensitivity and model performance.
	<b>Loss Collection Criteria</b>	Defined thresholds for collection of losses which may be material to capital calculations.

# ORM Framework Component Description



Element	Component	Component Description
Operational Risk Management & Monitoring	<b>Testing</b>	Use test demonstrating that the Operational Risk model is operationalized and embedded into business processes. Pre-implementation testing to ensure business and operational requirements are met.
	<b>Validation</b>	Review of business processes to provide management assurance that risk stakeholder needs are met.
	<b>Risk Mitigation Planning</b>	Identification, planning and completion of activities to reduce risks to acceptable levels.
	<b>Incident/Issue Management</b>	Approach and process to identify, capture and manage events and extreme events impacting an organization.
	<b>Customer Complaint Management</b>	Defined process and responsibilities for capture, reporting and resolution of customer complaints.
	<b>Change Control and Change Management</b>	Operational Risk assessments and approval and implementation processes to facilitate review and approval of new businesses, products and technology.
	<b>Third Party and Vendor Management</b>	Policies and processes for managing third party and vendor relationships and ensuring their business interactions with bank employees and customers align with an organization's risk appetite and applicable laws and regulations.
	<b>Business Continuity</b>	Business resiliency and continuity plans which ensure continued operation of critical business functions with limited losses in the event of severe business disruption.

# ORM Framework Component Description



Element	Component	Component Description
Operational Risk Reporting & Insights	<b>KRIs and Risk Limits</b>	Dynamic governance, monitoring, analysis and reporting to rapidly manage issues and strengthen process and control environment. Integrated risk profile that highlights key exposures and provides risk intelligence across business groups, processes and products, and supports a credible capital model. KRIs and Risk Limits should be focused on most relevant and strategically important risks.
	<b>Management Reporting and Escalation</b>	Processes to monitor and escalate risk to appropriate risk stakeholders throughout an organization. Defined processes/procedures to manage and escalate risk tolerance breaches and provide adequate risk transparency to the Board.
	<b>External Reporting</b>	Processes to fulfill stakeholder and shareholder reporting and risk transparency and to fulfill regulatory reporting requirements.

# ORM Framework Component Description



Element	Component	Component Description
Operational Data & Technology	<b>IT Architecture and Management</b>	Design, development and ongoing maintenance of centralized data repositories and robust technology infrastructure to support operational risk identification, measurement and monitoring.
	<b>Data Governance and Ownership</b>	Control mechanisms to develop common data definitions and establish data ownership and data quality standards.
	<b>Risk Data Aggregation</b>	Infrastructure and capabilities to ensure data is appropriately aggregated to provide timely and accurate representation of an organization's risk profile.
	<b>System/Tool Selection</b>	Selection of technology tools which meet business, financial and operational risk management requirements.
	<b>Disaster Recovery</b>	Programs in place to enable business continuity of key business processes in the event of a disaster.
	<b>Information Security</b>	Enterprise-wide, cross-functional programs highlighting roles of IT and the Business in managing threats and vulnerabilities in protecting employee and customer data.
	<b>Technology Enablement</b>	Implementation support for operational risk management technology.
	<b>Near Miss Data</b>	Process to analyze incidents which could potentially result in losses to identify required improvements to processes or controls to mitigate future losses.

*How do regulators define the Lines of Defense?*

*What are the primary objectives?*

1 <sup>st</sup> Line of Defense	2 <sup>nd</sup> Line of Defense	3 <sup>rd</sup> Line of Defense
<ul style="list-style-type: none"> <li>▪ Any organizational unit or function that is accountable for either credit risk, interest rate risk, liquidity risk, market risk, operational risk, compliance risk, strategic risk, legal risk or reputational risk and performs the following:                             <ul style="list-style-type: none"> <li>– Engages in activities designed to generate revenue or reduce expenses</li> <li>– Provides operational support or servicing to any organizational unit or function</li> <li>– Provides technology services to any organizational unit or function</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>▪ Any organizational unit that is independent from front line units and has responsibility for identifying, measuring, monitoring, or controlling aggregate risks</li> </ul>	<ul style="list-style-type: none"> <li>▪ Any organizational unit within a bank that is independent from front line units and risk management and designed to evaluate the adequacy of and compliance with policies, procedures, and processes established by the first line and independent risk management under the risk governance framework</li> </ul>
<ul style="list-style-type: none"> <li>▪ <b>Owns the risks</b> associated with their activities by assessing and managing risk</li> <li>▪ <b>Implements action plans</b> to strengthen risk management or reduce risk, given changes in the unit's risk profile</li> <li>▪ <b>Identifies, measures, monitors, reports, and controls</b> risk consistent with the Bank's risk appetite statement</li> </ul>	<ul style="list-style-type: none"> <li>▪ <b>Oversees the Bank's risk-taking activities</b> and assess risks independent of the front line units</li> <li>▪ <b>Designs a risk framework</b> commensurate with the Bank's risk appetite statement</li> <li>▪ <b>Identifies, measures, mitigates, monitors, and reports</b> the risk management practices of Business Groups, Geographies, IT Infrastructure, Support Functions, and Associates</li> </ul>	<ul style="list-style-type: none"> <li>▪ <b>Performs independent review</b> and objective assessments of adherence to policies, procedures, and internal controls</li> <li>▪ Conducts financial, operational, technology, risk management, compliance, and fiduciary <b>audits on a routine basis</b></li> </ul>

**Who performs risk management functions within the Lines of Defense?**

<b>Risk Type</b>	<b>1<sup>st</sup> Line of Defense</b>	<b>2<sup>nd</sup> Line of Defense</b>	<b>3<sup>rd</sup> Line of Defense</b>
<b>BSA / AML / OFAC</b>	Associates Business Groups Geographies BSA Operations / Enhanced Due Diligence	BSA / AML / OFAC Team Compliance and Regulatory Risk Team	Credit Risk Review Internal Audit
<b>Compliance</b>	Associates Business Groups Geographies IT Infrastructure Operations	Compliance and Regulatory Risk Team Legal	
<b>Credit</b>	Business Groups Geographies Underwriters Problem Asset Mgmt Collections	Credit Risk Team Risk Analytics	
<b>Market &amp; Liquidity</b>	Corporate Treasury	Market / Liquidity Risk Team	
<b>Operational</b>	Associates Business Groups Geographies IT Infrastructure Operations Finance Underwriters	Operational Risk Team Procurement Human Resources	
<b>Strategic / Reputational</b>	Business Teams IT Infrastructure Operations	Corporate Strategy Team Legal	

Governance / Oversight Committees

**Lines should be defined based on function performed not organizational alignment**

# Roles & Responsibilities

## Key Differences Between 1<sup>st</sup> and 2<sup>nd</sup> Lines of Defense

Area	1 <sup>st</sup> Line of Defense	Commonalities between 1 <sup>st</sup> & 2 <sup>nd</sup> Lines	2 <sup>nd</sup> Line of Defense
<b>Governance &amp; Culture</b>	<ul style="list-style-type: none"> <li>1<sup>st</sup> line <b>adheres</b> to Enterprise Risk Appetite Statement and <b>develops</b> Business Risk Appetite Statements</li> </ul>	<ul style="list-style-type: none"> <li>Both 1<sup>st</sup> and 2<sup>nd</sup> line monitor adherence to established risk limits, as applicable</li> </ul>	<ul style="list-style-type: none"> <li>2<sup>nd</sup> line <b>develops and administers</b> the Enterprise Risk Appetite Framework, Risk Management Framework, and <b>identifies risk liaisons</b></li> </ul>
<b>Policies &amp; Procedures</b>	<ul style="list-style-type: none"> <li>1<sup>st</sup> line <b>establishes business policies and / or procedures</b> to address risks / changes and <b>communicates</b> to all associates</li> </ul>	<ul style="list-style-type: none"> <li>Both 1<sup>st</sup> and 2<sup>nd</sup> lines <b>identify emerging risks</b> or changes and <b>monitor regulatory changes</b> in the industry</li> </ul>	<ul style="list-style-type: none"> <li>2<sup>nd</sup> line <b>interprets</b> applicable laws, regulatory guidance, etc. and <b>establishes corporate policies</b> and <b>provides guidance</b> to business policies</li> </ul>
<b>People &amp; Skills</b>	<ul style="list-style-type: none"> <li>See next column</li> </ul>	<ul style="list-style-type: none"> <li>Both 1<sup>st</sup> and 2<sup>nd</sup> lines ensure associates <b>have necessary skills, adequate training</b> to fulfill responsibilities, and continuously assess staffing levels</li> <li>Both 1<sup>st</sup> and 2<sup>nd</sup> lines develop <b>risk performance metrics</b> and <b>succession plans</b> for key personnel</li> </ul>	<ul style="list-style-type: none"> <li>2<sup>nd</sup> line assists with <b>content creation and delivery</b> of training</li> </ul>



# Roles & Responsibilities

## Key Differences Between 1<sup>st</sup> and 2<sup>nd</sup> Lines of Defense (Cont'd)

Area	1 <sup>st</sup> Line of Defense	Commonalities between 1 <sup>st</sup> & 2 <sup>nd</sup> Lines	2 <sup>nd</sup> Line of Defense
<b>Monitoring &amp; Testing</b>	<ul style="list-style-type: none"> <li>▪ 1<sup>st</sup> line monitors adherence to policies and / or procedures through <b>real time</b> (Quality Control) and <b>post process testing and / or monitoring</b> (Quality Assurance) within respective areas</li> <li>▪ 1<sup>st</sup> line <b>escalates issues</b> identified through QA / QC to impacted areas / businesses</li> <li>▪ 1<sup>st</sup> line <b>monitors business risk</b> through 1<sup>st</sup> Line Risk Assessments</li> <li>▪ 1<sup>st</sup> line <b>executes</b> risk management programs</li> <li>▪ 1<sup>st</sup> line <b>escalates risks / issues</b> and <b>develops corrective action plans</b> to mitigate risk</li> </ul>	<ul style="list-style-type: none"> <li>▪ <b>Both 1<sup>st</sup> and 2<sup>nd</sup> lines respond to regulatory requests</b></li> </ul>	<ul style="list-style-type: none"> <li>▪ 2<sup>nd</sup> line establishes select enterprise wide testing and / or monitoring programs and performs <b>targeted assessments of higher risk processes</b></li> <li>▪ 2<sup>nd</sup> line <b>develops framework</b> for monitoring risk, <b>provides effective challenge</b> to the 1<sup>st</sup> line and <b>monitors aggregate risk levels</b></li> <li>▪ 2<sup>nd</sup> line <b>develops and administers</b> risk management programs 2<sup>nd</sup> line <b>monitors closure</b> of higher risk issues</li> </ul>
<b>Information Reporting &amp; Technology</b>	<ul style="list-style-type: none"> <li>▪ 1<sup>st</sup> line <b>establishes reporting routines, owns data quality, and is responsible for technology system recoverability</b></li> </ul>		<ul style="list-style-type: none"> <li>▪ 2<sup>nd</sup> line <b>monitors aggregate risk profiles, communicates regulatory data retention requirements, and monitors disaster recovery testing</b></li> </ul>

# Roles & Responsibilities

## Key Differences Between 1<sup>st</sup> and 2<sup>nd</sup> Lines of Defense (Cont'd)

Area	1 <sup>st</sup> Line of Defense	Commonalities between 1 <sup>st</sup> & 2 <sup>nd</sup> Lines	2 <sup>nd</sup> Line of Defense
<b>Risk Management Processes</b>	<ul style="list-style-type: none"> <li>▪ 1<sup>st</sup> line <b>assesses risk impacts</b> of changes to the organization</li> <li>▪ 1<sup>st</sup> line (Business) <b>develops business requirements</b> and (Ops &amp; Tech) translates into a functional design</li> <li>▪ 1<sup>st</sup> line (Business) <b>confirms business requirements are fulfilled</b> and (Ops &amp; Tech) <b>tests design specifications</b> against business requirements</li> <li>▪ 1<sup>st</sup> line <b>analyzes client risk profiles</b> to confirm alignment with risk appetite</li> <li>▪ 1<sup>st</sup> line <b>establishes controls to prevent operational losses</b></li> <li>▪ 1<sup>st</sup> line <b>executes</b> vendor management &amp; 3<sup>rd</sup> party compliance programs</li> </ul>	<ul style="list-style-type: none"> <li>▪ Both 1<sup>st</sup> and 2<sup>nd</sup> lines <b>monitor customer complaints</b> and evaluate new initiatives / new products</li> </ul>	<ul style="list-style-type: none"> <li>▪ 2<sup>nd</sup> line <b>provides subject matter guidance</b> on potential impacts of changes and <b>reviews requirements</b> to ensure risks are addressed (including regulatory requirements)</li> <li>▪ 2<sup>nd</sup> line <b>monitors enterprise product suite</b> to ensure adherence to <b>regulatory / corporate guidelines</b></li> <li>▪ 2<sup>nd</sup> line reviews <b>operational loss events</b></li> <li>▪ 2<sup>nd</sup> line <b>develops and administers</b> vendor management and 3<sup>rd</sup> party compliance program</li> </ul>
<b>IT Service Delivery</b>	<ul style="list-style-type: none"> <li>▪ 1<sup>st</sup> line <b>implements policies and process</b> to address data accessibility, quality, and security</li> <li>▪ 1<sup>st</sup> line <b>establishes and maintains</b> access control and software management policies and procedures and manages service availability to defined targets</li> <li>▪ 1<sup>st</sup> line <b>maintains procedures to measure, analyze, and manage</b> incidents and problems</li> </ul>		<ul style="list-style-type: none"> <li>▪ 2<sup>nd</sup> line <b>provides oversight and effective challenge</b> of incident management, data management, and data classification</li> <li>▪ 2<sup>nd</sup> line <b>performs IT Compliance assessments</b> to evaluate key vulnerabilities</li> </ul>

# Roles & Responsibilities - Perspectives on the Three Lines of Defense

1

**Three Lines of Defense is a useful framework for defining the approach to risk governance.** However, it is not always well understood.

2

**Establishing ownership and management of risk within the business is essential to successful implementation of the three Lines of Defense.**

3

Three Lines of Defense is best seen as a series of guiding principles which drive the establishment of roles and responsibilities of individuals and functions that are compatible within a coherent structure. **There is not a singular right answer and structure may vary across organizations, businesses, and risk types.**

4

The failings attributed to the model as a result of the financial crisis were failings of implementation with, in particular, a failure to achieve #2 above but also a failure of the 2<sup>nd</sup> line to apply its veto to excessive risk taking. **Most banks have not yet evolved to a position where risk ownership and management are embedded in the 1<sup>st</sup> line**

5

Most banks have significantly increased headcount in the 2<sup>nd</sup> and 3<sup>rd</sup> Lines of Defense as they aim to enhance their risk management and control frameworks, whereas, **it is expected that embedding risk ownership and management in the 1<sup>st</sup> line successfully should result in a reduction in the resources required in 2<sup>nd</sup> and 3<sup>rd</sup> line functions.**

6

**The processes by which the 1<sup>st</sup> line takes and manages risk must be transparent to facilitate effective oversight and control** by the 2<sup>nd</sup> line and assessment of the overall effectiveness of the combination of the 1<sup>st</sup> and 2<sup>nd</sup> lines by the 3<sup>rd</sup> line.

# Risk Appetite Statement & 1<sup>st</sup> Line Risk Assessment

## Key Components of Effective Risk Management

Framework

### Risk Appetite Framework

*Provides overarching methodology and framework for developing, effectively utilizing, and maintaining the Enterprise and Business Unit Risk Appetite Statements*

Key Components

#### Board of Directors Risk Appetite Statement

*Enterprise-level statement that defines the amount of risk the bank is willing to accept to achieve its strategic objectives, in terms of its impact on Earnings, Capital, Liquidity and Stakeholder Confidence*

#### Risk Category Level Statements

*Details the Board of Directors Risk Appetite Statement by the 8 key risk categories to further define the appetite for each risk type*

#### Business Unit Risk Appetite Statements

*Translates the Board of Directors Risk Appetite Statement and the Risk Type Statements down to the level at which strategy is developed (where possible)*

#### Key Risk Indicators

*Monitors risk by providing an early indication that risk levels are increasing, so that appropriate action plans to mitigate risk can be taken*

Performance reporting against Business Line Risk Appetite Statements (RAS) and Key Risk Indicators are key components of the 1<sup>st</sup> Line Risk Assessments

### 1<sup>st</sup> Line Risk Assessments

*Provide a consistent method of viewing and reporting on risk profile in the 1<sup>st</sup> Line of Defense. Method for reporting performance against business line risk appetite evaluating risk profiles of the business*

# Risk Appetite Statement & 1<sup>st</sup> Line Risk Assessment

## Risk Appetite Statement

### Common Challenges

- Linking Risk Appetite Statement to overall corporate strategy/business objectives and embedding a strong **risk culture**
- **Aligning** business strategy, risk profile, and capital plan with risk appetite
- Effectively **cascading Risk Appetite throughout the firm**, from enterprise level, to risk statement level, to LOB level
- **Capturing material types of risk** facing the firm, including those qualitative elements of risk which are often not easily measured (e.g., reputation risk)
- Designing Risk Appetite Statements to help drive **decision making** based on risk
- Using risk appetite proactively to **consider business opportunities and strategic options**
- Ability to **identify and aggregate risk** within and across legal entities, business lines, products and services, and geographies

### Risk Appetite Statement Critical Components

- Risk Appetite Statements are **forward-looking** and tied to strategy and core business objectives
- Business strategy and budget plans are aggregated and aligned to Risk Appetite via an **iterative process**
- **Training and communication** tie risk appetite to day-to-day decision making
- Risk Appetite **contains both qualitative components and quantitative limits** (Metrics/tolerances help **quantify risks**)
- Both **OCC and Federal Reserve Categories of Risk** are included within the RAS
  - Compliance, Credit, Interest Rate, Legal, Liquidity, Operational, Price, Reputational, Strategic
- **Quantitative limits** should incorporate sound stress testing processes
- The suite of risk limits should **include concentration risk** limits
- Use **common, easy to understand language**
- Include metrics/tolerances which serve as **early-warning indicators** of emerging risk
- Incorporate **robust limit breach protocols**, including escalation, reporting, and remediation, as appropriate

# Risk Appetite Statement & 1<sup>st</sup> Line Risk Assessment

## Tools to Measure Operational Risk

		<b>How the Tool Informs Operational Risk</b>
<b>Risk and Control Self-Assessment (RCSA)</b>	Operational risk tool to document key business processes, identify key risks and controls (primarily operational) and measure the levels of inherent / residual risk within key processes	Measures the inherent and residual risks of the business and identifies areas of high operational risk and control adequacy. High risk processes can be monitored through KRIs / KPIs
<b>Operational Metrics</b>	Key Risk Indicators (KRI) or Key Performance Indicators (KPIs) to monitor current risk levels in the business or forecast when processes / controls may be under stress and could result in a failure	Metrics and tolerances monitor levels of risk, indicate higher risk areas, and trigger action when risk levels are rising
<b>Operational Losses</b>	Quantifies operational loss events that have occurred and identifies thematic or similar type events	Quantifies historical operational losses within the business requiring root cause analysis
<b>Root Cause Analysis</b>	Analysis of large operational losses to identify opportunities to enhance process / controls to prevent future operational losses	Identifies the root cause of operational losses and alerts the business of high risk areas / processes
<b>Scenario Analysis</b>	Development of hypothetical scenarios to measure the likelihood and severity of this event. This type of exercise also identifies downstream impacts and stresses business continuity plans	Analyzes the potential outcomes of various hypothetical situations and informs capital modelling for operational risk
<b>New Initiatives Risk Assessments / Other Governance</b>	Identifies significant changes to the organization likely impacting existing processes / controls prior to implementation	Analyzes potential operational risks associated with change to identify increasing risk in people, process, and technology

# Risk Culture

## Risk Culture Basics

### **What is Risk Culture?**

- Attitudes within the firm regarding taking and managing risks
- Culture varies between firms, but can also vary between businesses at the same firm
- Culture and attitude change over time

### **How is Risk Culture developed?**

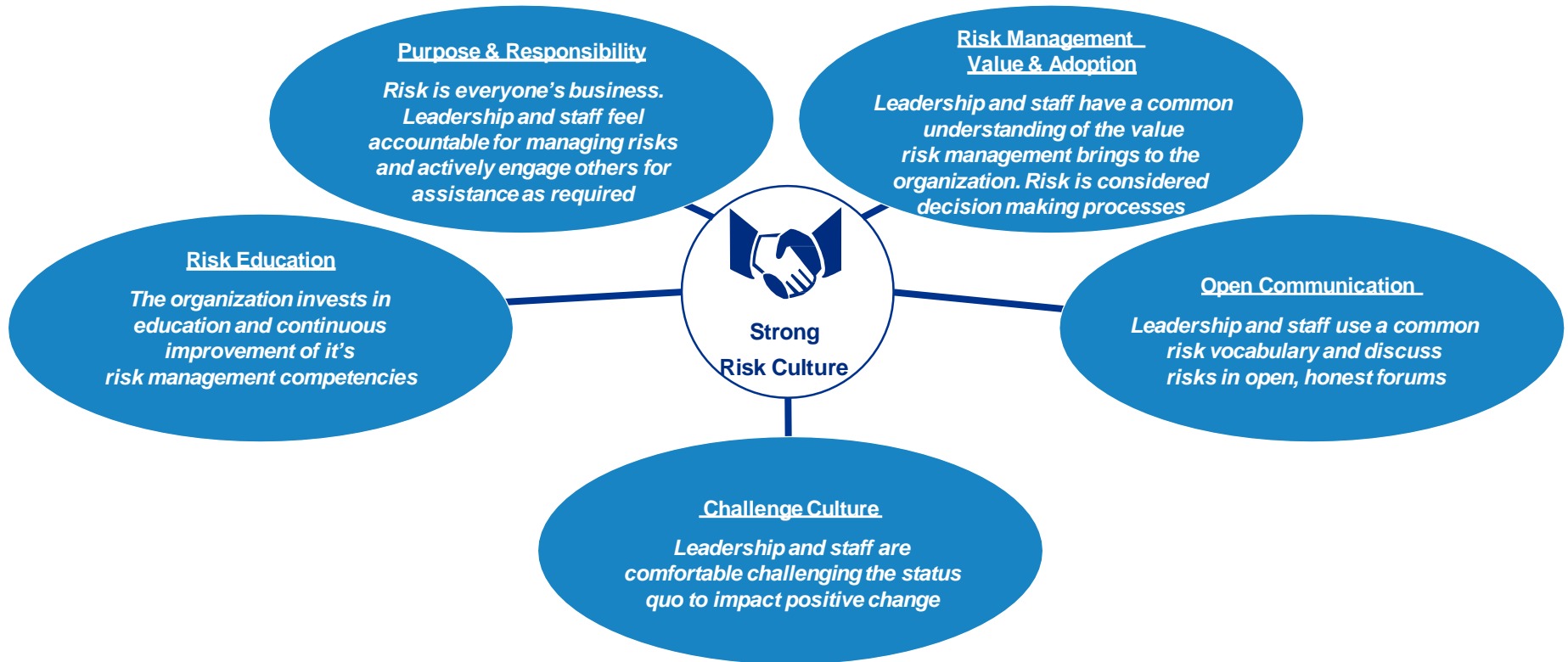
- **Formally-** Policies, codes of conduct, codes of ethics, statements of values, etc.
- **Informally-** Behaviors that are condoned, encouraged, or rewarded. Behaviors observed in senior management. Consistencies or inconsistencies between official statements and actual results, as well as incentives and desired behaviors.

### **What does culture need to be?**

- Sensible, informed risk taking is part of doing business
- There is transparency and consistency in actions, communications, and incentives
- There is active and acknowledged ownership of risk by risk generators
- Risk generators are held accountable for management of their risks
- There is open communication – no blame, no shame
- Mistakes = Learning Opportunities

***“...if there isn’t an appropriate risk culture in the first Line of Defense, no amount of money spent in the second and third Lines of Defense can make up for it in managing risk and protecting the company...” -paraphrase, Senior Supervisors Group (FSB)***

# Risk Culture - What Drives Culture?



- **Tone at the top** - Board and Senior management demonstrate strong risk culture in communications and behaviors
- **Risk in decision making** - Risk considerations are assessed when making business decisions
- **Response and reinforcement** - Leadership and staff are encouraged to raise potential issues rather than “sweep under the rug”
- **Alignment of compensation** - Compensation and incentives link to risk management performance, not only production volumes



# ORM Focus Areas

- “Effective” Operational Risk Management
- Cyber risk
- Third party risk management (lifecycle view)
- New Products (lifecycle view)
- Model risk management
- Risk Culture, Conduct, and Behavior
- Front line ownership of risk – Second line oversight
- Risk and Control Self Assessment (RCSA) linked to forward looking KRIs
- Front line quality assurance
- Front line operational risk deep dives (product, process, platform)



[kpmg.com/socialmedia](https://kpmg.com/socialmedia)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDPPS 591094

The KPMG name and logo are registered trademarks or trademarks of KPMG International.