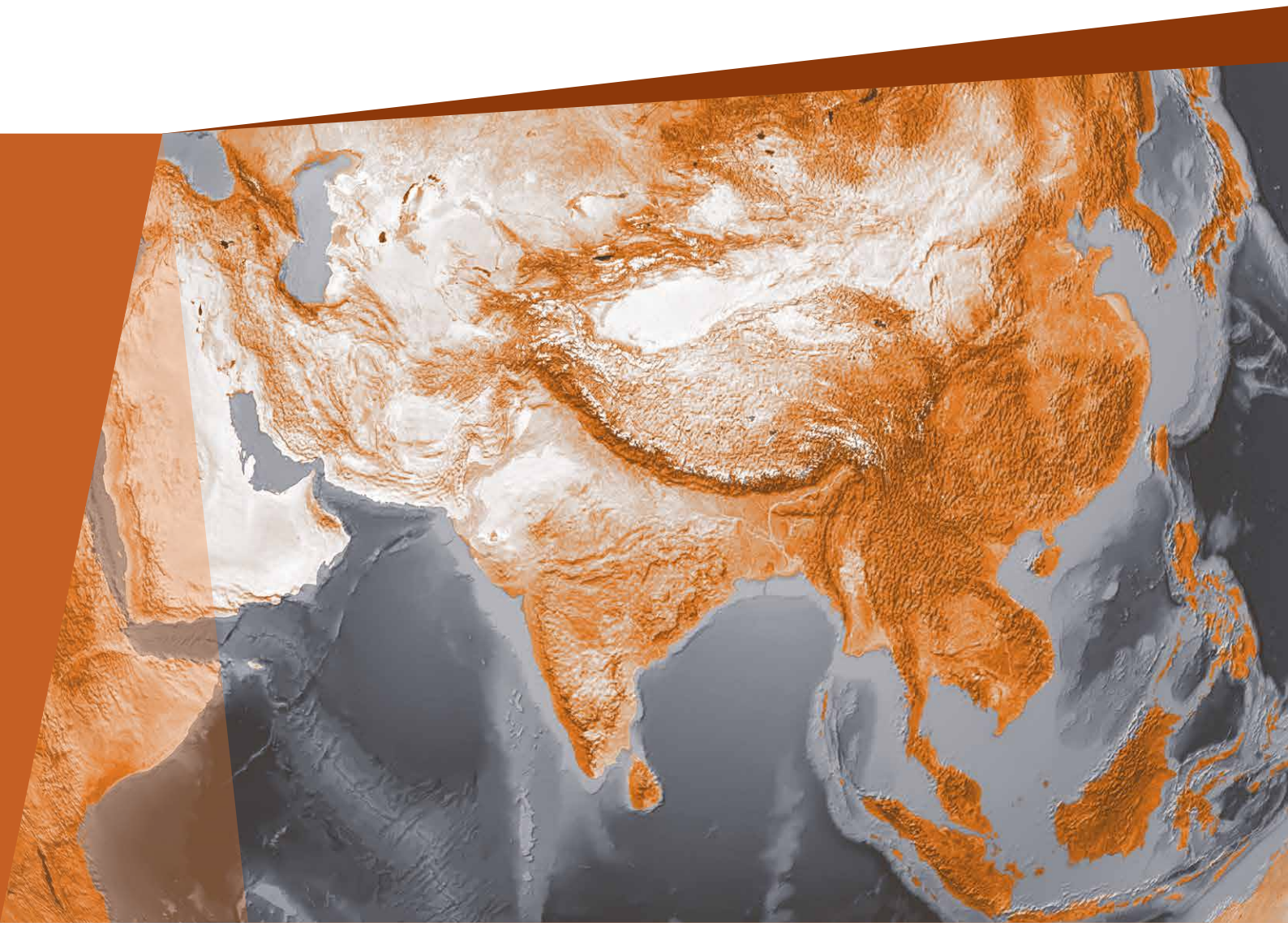
OLIVER WYMAN

Financial Services



ASIA PACIFIC FINANCE AND RISK SERIES

STREAMLINING RISK, COMPLIANCE AND INTERNAL AUDIT

LESS IS MORE

MARSH & McLENNAN COMPANIES

INTRODUCTION: TODAY'S RISK LANDSCAPE

Since the financial crisis of 2007–2008, the financial services industry has been beset by a series of major operational, compliance and conduct-related events which have highlighted fundamental failures in management, internal controls and risk governance.

Many of these failures were embedded within the firms' operations pre-crisis due to expanding revenue pools, poorly aligned incentives and culture which created an environment of aggressive risk-taking heading for a fall. Warnings from Risk, Compliance and Internal Audit were often ignored by senior management in the firms' drive for ever higher profit margins.

Exhibit 1: Series of major control failures in Financial Services

$1 TN
In value of S&P stocks lost in 15 minutes due to glitch in algorithms (US Flash Crash, 2010)

$7.2 BN
Loss due to rogue trading (Jerome Kerviel, 2008)

$6.2 BN
Loss due to rogue trading (London Whale, 2012)

>$4.7 BN
Fines levied on banks due to LIBOR manipulation; Barclays Chairman and CEO forced to resign whilst 11 other banks currently being investigated by the EC & US FDIC (2012–ongoing)

>$1 BN
Fines levied on banks for breaking US sanctions against Iran, Cuba, Sudan and Libya (2009–2012)

$13 BN
Fines levied on a single bank due to mis-selling of mortgage-backed securities (2013)

$1.9 BN
Fines levied on a single bank due to money laundering (2012)

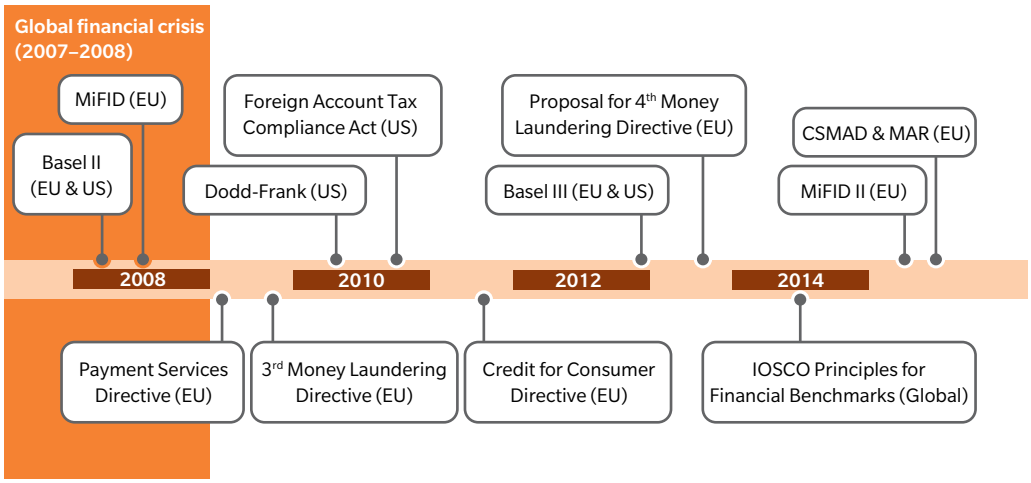
>$9.3 BN
Fines levied on banks in UK due to Payment Protection Insurance (PPI) mis-selling (2011–ongoing)

These events have triggered a fresh wave of regulatory reforms in Europe and US, as regulators focus their efforts on ensuring greater oversight and accountability by senior management.

Regulators are currently reviewing the adequacy of operational risk capital requirements for financial services firms in the light of the financial crisis[1]. Furthermore, regulators are enforcing the concept of personal liability with the introduction of criminal sanctions on certain financial misdemeanours through such acts as the US Dodd-Frank Act and European Criminal Sanctions for Market Abuse Directive (CSMAD).

1 BCBS 291 Revision to operational risk – simpler approaches (Oct 2014 consultation paper); BCBS 292 Review of Principles for Sound Management of Operational Risk (Oct 2014); BCBS 298 Reducing excess variability in banks' regulatory capital (Nov 2014).

Exhibit 2: Wave of regulations



Note: Regulations included in the above illustrations are not a comprehensive list of regulations influencing the global financial services industry. Timeline indicates when a regulation was or is due to be implemented.

Whilst Asian markets have been relatively sheltered in recent years – firms are braced for an oncoming storm as Asian regulators look to Europe and US for inspiration in order to avoid similar crises. In addition, regulators are considering greater regulatory coordination and cooperation across national jurisdictions in order to combat risks which are increasingly borderless.

Regulators are demanding more from Boards and senior management, who are in turn demanding more from their risk and control functions to ensure greater control and oversight of their key risks.

Risk, Compliance and Internal Audit functions need to evolve quickly to provide adequate insight to regulators and senior management.

KEY CHALLENGES

Globally, firms are increasing spending on controls – with at least $50 BN spent on risk and compliance initiatives in response to regulatory and management pressure. However there has been little observed benefits thus far, as evidenced by the observed trend in operational risk losses – which have gone up by at least five-fold from 2010–2013. The severity of operational risk events has increased; not just due to regulatory fines but also due to reputational and legal impacts – where individuals may be criminally prosecuted and senior management forced to step down.

As senior management and Boards grapple with these issues – they face the following challenges:

1. Unclear scope of mandate and roles: Historically the scope and mandate for Risk, Compliance and Internal Audit functions were not clearly delineated; with multiple overlaps with the business, each other and other control functions. This often led to duplication of work or gaps in coverage. In addition, the roles between second (Risk, Compliance) and third line of defence (Internal Audit) were often blurred – with Internal Audit being involved in advisory and other activities more typically conducted by the second line.
2. Uncoordinated/inconsistent processes: Many institutions lack a common taxonomy that is consistently applied across the institution as well as consistent processes for risk identification, assessment and mitigation across the different control functions. This often resulted in increased burden on the businesses due to duplicated or contradictory requests. It also made it difficult to share information across the control functions.
3. Multiple overlapping reports to senior management: Many institutions highlight the issue of having multiple reports providing similar content to senior management, which are often backward-looking with insufficient focus on emerging risks. In addition, there is typically little qualitative insight or actionable recommendations for senior management to act on – making it difficult for senior management to have sufficient line of sight of the key risks and controls within the businesses.
4. Lack of skilled resources: Many institutions highlight that the burdens of running a modern Risk, Compliance or Internal Audit function are so complex that functional specialty is often developed at the cost of business understanding. Hence there is often limited business or specialist expertise to provide sufficient challenge to the businesses. In addition, there is typically little or no expertise in emerging risks (e.g. Anti Money Laundering (AML), conduct, cyber security, etc.). Moreover, the control functions are typically centralised with insufficient FTEs embedded within the business units to manage and mitigate key risks.
5. Fragmented systems: Many institutions lack a centralised system to enable information sharing or follow-up due to historical legacy of multiple databases/spreadsheets/documents which are largely manual. In addition, there are huge challenges to integration due to fragmented and non-standardised data; exacerbated by lack of consistent application of a common taxonomy and processes. Whilst some institutions are moving towards an integrated Governance, Risk and Compliance (GRC) system; the GRC systems available in the industry are still relatively less mature compared to other banking application systems and require greater effort in implementation.

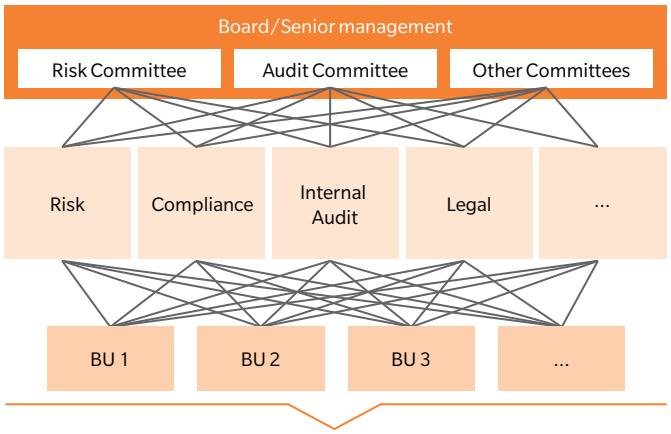
Whilst the challenges are common across both sophisticated and developing institutions, the key drivers differ. Most financial institutions in sophisticated markets are focused on the idea of **"compliance at any cost"** – which has led to a proliferation of multiple individual control frameworks with isolated views on specific risks and controls within their particular mandate. In contrast, financial institutions in developing markets typically start from a low base with little investment spent on their risk and control functions compared to the frontline.

Given resource and budgeting constraints, leading institutions are focusing on **"control optimisation"** – a top-down approach focusing on the largest risk and control issues to provide clarity and direction for achieving real risk management and more valuable control improvements. Whilst this is a multi-year task, initial benefits include:

- Increased transparency for senior management
- Ability to demonstrate better risk management capabilities to regulators
- Approximately 30% decrease in number of control tests required
- Reduction of operational losses/errors ranging from approximately 0.3%–0.8% of total revenues

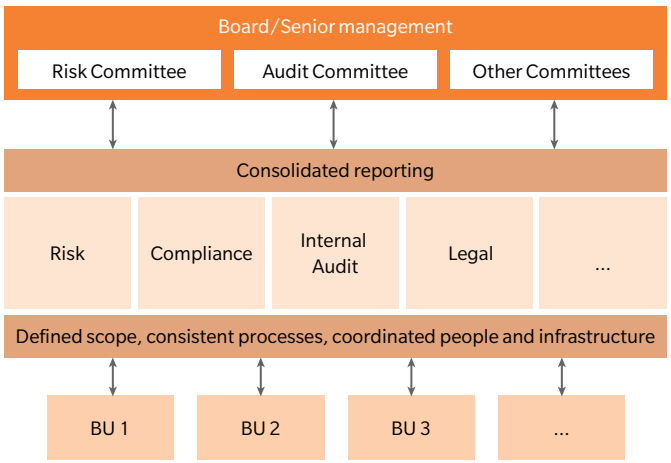
Exhibit 3: Compliance at any cost vs. control optimisation

COMPLIANCE AT ANY COST



- Description
  - Multiple, overlapping control functions and frameworks operating in silos
- Issues
  - Lack of clarity on control functions' scope and mandate
  - Senior management confusion and lack of clarity on actual top risks
  - Fragmented systems and uncoordinated processes

CONTROL OPTIMISATION



- Description
  - Optimised control framework through selective alignment or integration of risk and control frameworks and methodologies
- Benefits
  - Aligned scope and mandate across control functions
  - Provide senior management comfort in ensuring holistic approach towards management of top risks and controls
  - Potential cost-savings due to streamlining of required controls, processes or systems
  - Potential loss reductions due to integrated approach

NEXT GENERATION TARGET STATE: CONTROL OPTIMISATION

Regulatory compliance initiatives provide much useful structure for leverage including: common language, risk assessments, detailed and comprehensive control documentation, ongoing monitoring activities, etc. These could be selectively joined up across various risk and control functions to streamline existing processes and frameworks. Leading institutions are looking to simplify and optimise their existing control frameworks across four key dimensions:

1. Aligned scope and mandate
2. Aligned methodologies and processes
3. Consolidated Management Information (MI) and actionable reporting
4. Coordination of people and infrastructure

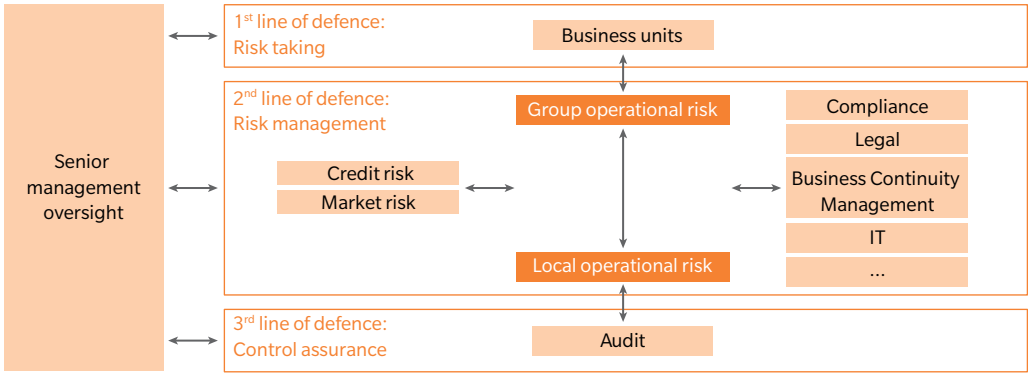
1. ALIGNED SCOPE AND MANDATE

Operational risk covers a wide range of non-financial risks[2]; however most Operational Risk functions lack the specialist resources to manage all of these risks. Historically, many institutions have delegated management of specific operational risks to specialist functions (e.g. Compliance, Legal, Information Technology (IT), etc.), whilst Operational Risk functions tended to focus on loss data collection, risk self-assessments, scenario analysis and capital modelling.

Given the rise in importance of operational risks, leading institutions are moving away from the traditional role of Operational Risk towards a more pro-active role as a facilitator to help coordinate the management of operational risk across the institution. In addition, both regulators and senior management are demanding more from their risk and control functions in terms of providing objective, holistic and timely advice on risks taken by businesses not only on what "has been done" but forward-looking views on what "should be done".

2 Basel defines Operational Risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk". Many compliance and conduct-related events also stem from operational risk events due to control failures (e.g. AML/sanctions breaches, rogue trading, mis-selling, etc.).

Exhibit 4: Interactions across the 3 lines of defence, roles and touch points



1st line of defence

- Business units
  - Seek best risk/return trade-offs to meet Group objectives
  - Full ownership of day-to-day risk-taking
  - Identify, assess, manage, mitigate and report on risk

2nd line of defence

- Operational risk
  - Overall view of all operational risks
  - Ensure consistent framework for identifying, measuring and monitoring operational risk
  - Facilitate management of operational risk
- Specialist functions
  - Specialist oversight and ownership of specific operational risks (e.g. Compliance, IT, etc.)
  - Create policies, educate business units and ensure firm-wide management of these specific risks

3rd line of defence

- Audit
  - Independent review of adherence to risk and control policies, mandates and guidelines
  - Identify improvement opportunities

Key touch-points

- Risk and control self-assessments, monitoring and reporting of risk/control issues and actions
- Risk and control assessments, monitoring and reporting of risk/control issues and actions
- Risk identification and control improvements, follow-up on mitigation actions

KEY AREAS TO DEFINE

- What is in scope vs. not in scope: Clear delineation of roles and responsibilities in processes related to a specific risk. For example, there has been (and still is, to some extent) relative lack of clarity with regards to the roles and responsibilities of Operational Risk and Compliance functions with regards to risks of regulatory non-compliance, such as AML, Know Your Client (KYC), sanctions, etc. In addition, recent regulatory developments in Europe around conduct risk have also caused firms to create Conduct Risk functions – which have many overlapping responsibilities with Operational Risk and Compliance. In addition, there has been increasing regulatory push for Internal Audit functions to conduct risk-based reviews and better understanding of risks and controls.
- Touch-points and rules of engagement with other units: For each risk, it is useful to determine which control function would take the lead in which process, the frequency of interactions with the business units as well as coordination and communication with other control functions in order to help streamline potentially risk and control processes.

2. ALIGNED METHODOLOGIES AND PROCESSES

A common taxonomy is often the first and most crucial step as it provides a common language as well as a consistent and systematic approach to identification, monitoring and management of risks across the firm.

Exhibit 5: Common taxonomy

BENEFITS OF IMPLEMENTING A COMMON RISK TAXONOMY

1. Systematic approach
- Provide a systematic approach for risk management, ensuring comprehensiveness and common structure
- Enhance the effectiveness of risk analysis and risk mitigation
  - Scope is clearly defined
  - Inputs from multiple businesses, branches can be aggregated (as names/definitions of risks are aligned)
- Facilitate identification, monitoring and management of risks common across all branches (as names/definitions of risks are aligned)

2. Business understanding
- Allow business units to better understand sources of their risks
- Provide structure to the data collected

3. Common languages
- Allow effective communication across control functions (e.g. Risk, Compliance and Audit, etc.)
- Provide a communication channel on emerging risks and their definitions across the bank

However, there are a number of common pitfalls that many firms experience:

- Lack of consistent taxonomy definition
- Lack of consistent application across all framework components
- Confusion between taxonomy vs. risk and control registers
- Unclear link to governance processes

These pitfalls can be mitigated through having a strong top-down coordinated approach across all control functions in designing a common risk taxonomy that is consistent and comprehensive, with linkages to other risk and control framework components clearly defined.

Once a consistent taxonomy has been defined, the next step is to determine a consistent approach to identifying and assessing risks and controls through the use of similar methodologies to enable greater ease in information sharing where required. Whilst it is not feasible (nor necessarily desirable) to have full alignment of methodologies across all control functions due to the differentiation in focus of risk; leading institutions are moving towards greater alignment through having a more risk-based approach for identifying and assessing risks. Firms are also coordinating the timing of different Operational Risk, Compliance and Internal Audit processes to reduce workload on businesses where feasible (e.g. combining requests to businesses or providing results to other control functions to prevent duplication of requests).

In addition, majority of firms noted that it is important to maintain ongoing dialogue between Operational Risk, Compliance and Internal Audit functions to facilitate learning from each other on an operational level and to enable greater information sharing.

3. CONSOLIDATED MI AND ACTIONABLE REPORTING

Consolidated reporting can help streamline overlapping areas of reporting and significantly improve degree of coordination required across businesses, control functions and Internal Audit.

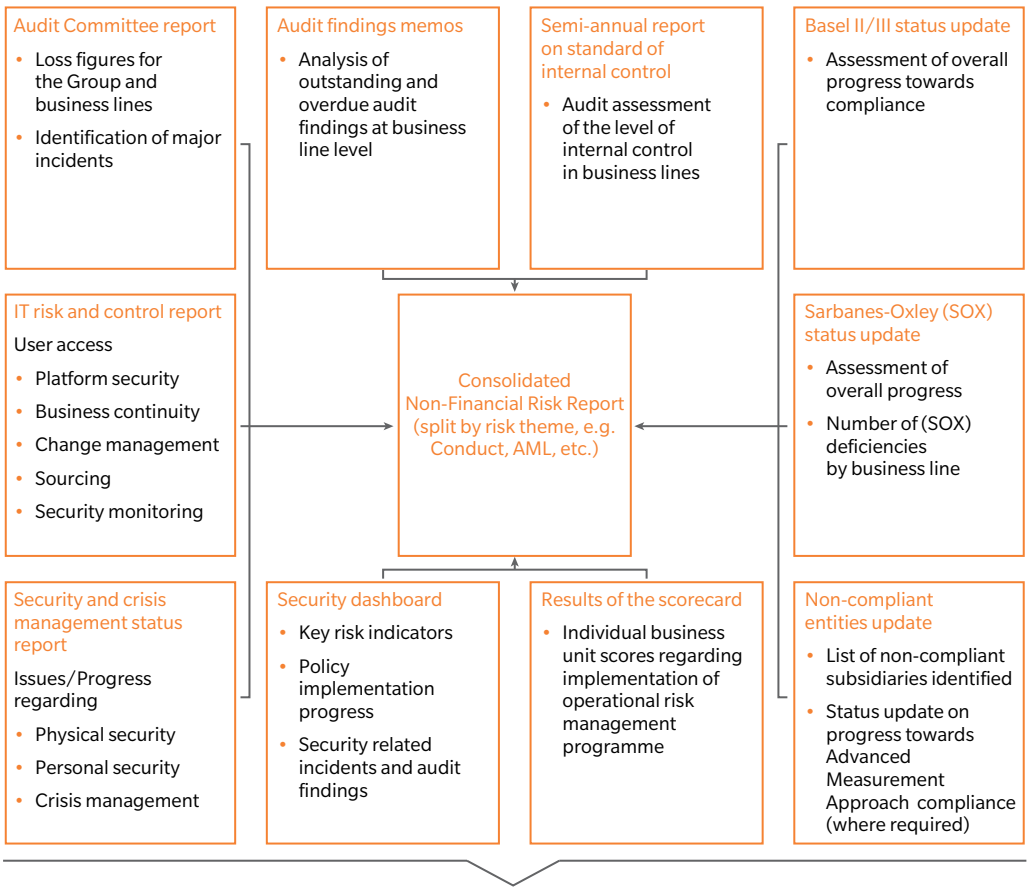
Good reporting practices and well-designed reports should help to aggregate and analyse data to answer core questions such as:

- How much risk is the bank taking?
- Where is the risk generated?
- How is it mitigated?

More effective communication would lead to increased responsiveness as threats to the bank can be detected and mitigated earlier through: highlighting key messages, comparing results against benchmarks, scenario and sensitivity analyses, showing early warning indicators and analysing trends, highlighting lessons learnt and suggesting actions to be taken.

Exhibit 6: Consolidated reporting

DISGUISED CLIENT EXAMPLE: UNDERLYING REPORTS USED AS SOURCES FOR EXECUTIVE COMMITTEE DASHBOARD



Key questions addressed

- How much risk is the bank taking?
- Where is the risk generated?
- What are the key regulatory requirements and control issues?
- How is it mitigated?

4. COORDINATION OF PEOPLE AND INFRASTRUCTURE

PEOPLE

Whilst the majority of firms have embedded FTEs within business units for Operational Risk and Compliance and specialist audit teams to review specific regulatory issues; the higher bar set by regulators and senior management for Operational Risk, Compliance and Internal Audit functions demand a greater variety in skills and competencies than previously. Leading institutions are increasing spend on Risk, Compliance and Internal Audit resources both at Group and business unit level, as well as looking to close identified gaps through the following methods:

- Rotation programs: Rotation programs spanning across the three lines of defence are considered useful as it transfers not only knowledge from the business to control functions (Risk, Compliance and Internal Audit), but also helps create awareness about risks and controls (and related language, tools and processes) within the business
- Recruiting: Risk and compliance staffing budgets are also expected to expand in line with the increased regulatory and management requirements, with many institutions looking to invest in specialist expertise such as: AML, conduct risk, cybersecurity, etc.
- Training: Institutions are also looking into improving their training programmes in order to ensure that there is not only greater awareness of key risks and controls but also a focus on cultivating a strong risk culture

In addition, many leading institution are also ensuring that their risk and control staff are actively engaged in regulatory or industry discussions in order to help shape future regulatory requirements or to share experiences and learn from other industry participants.

INFRASTRUCTURE

A common IT platform can provide tremendous value through providing a centralised risk and controls database which enables greater information sharing amongst control functions of policies, controls and risk assessments and issues identified. In addition, it supports unified tracking and monitoring of issues as well as enabling creation of standardised reporting templates/dashboards. It also reduces the effort required for reconciliation since it is sourced from a centralised database.

CONCLUSION

In summary, with the rise in increasing complexity of risks and higher expectations from both regulators and senior management, many leading institutions are looking to simplify and optimise their existing control frameworks in order to improve control effectiveness.

Whilst leading institutions in Europe and US are looking to upgrade their control functions along the dimensions described earlier, many are hampered by large existing incumbent control functions and new upcoming functions as a result of the recent wave of regulatory requirements. In contrast, many institutions in Asia and other emerging economies typically start from a low base and hence have greater scope for a more drastic re-development of their control functions as it were.

Strong leadership and support is required from both Board and CEO to drive through the necessary changes.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

ASIA PACIFIC
+65 6510 9700

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

AUTHORS' CONTACT INFORMATION

Christian Pedersen
Partner and Head of Finance and Risk Practice, Asia Pacific
+65 6510 9700
christian.pedersen@oliverwyman.com

Cheah Wei Ying
Manager, Finance & Risk Practice
+65 6510 9700
weiying.cheah@oliverwyman.com

www.oliverwyman.com

OLIVER WYMAN