GATEKEEPING CONSULTING

Good Governance and Compliance Culture:

The Foundation of Effective ML/TF/PF Risk Management

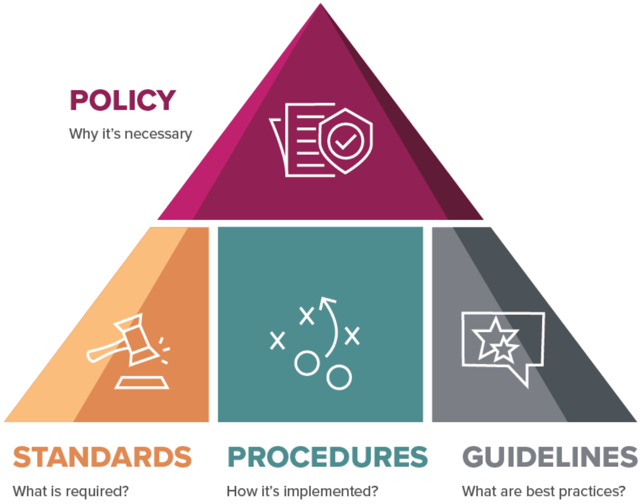
"AML effectiveness is not so much a compliance problem, as that it is a governance outcome."

Ronald F Poll

Good Governance and Compliance Culture:

The Foundation of Effective ML/TF/PF Risk Management

Most AML/CFT failures are not because there is a lack of frameworks, policies, or compliance functions.



The issue often is not structural, but relational.

How do **governance, management, and compliance interact** with each other to manage risk effectively?

This presentation explores that interaction and how it determines real-world effectiveness.

The Reality: Why Failures Still Occur

Many institutions have:

- RMCPs in place
- Compliance teams established
- Monitoring systems operational
- Board reporting in place

Yet still experience:

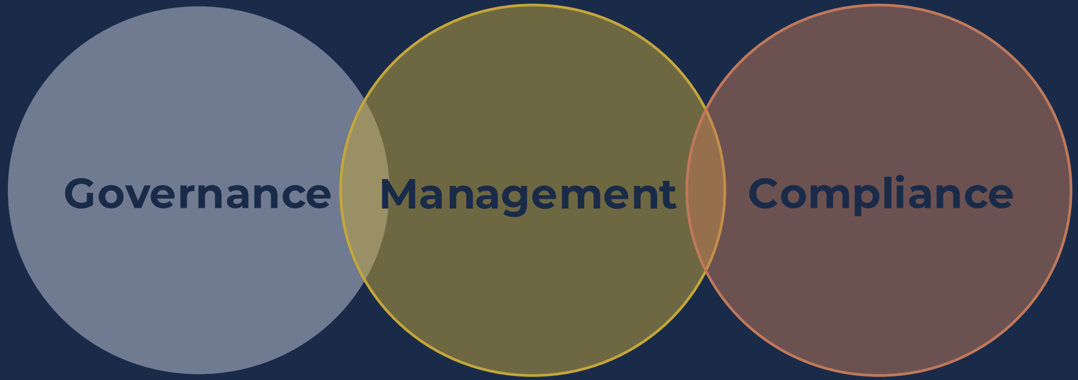
- Control breakdowns
- Delayed escalation response
- Misaligned risk appetite
- Regulatory findings

Key insight: Having a compliance framework does not guarantee effective risk management. The gap is not structural. It is relational.

The Core Question:

If frameworks exist, why do failures still occur?

The answer usually lies in how three components interact:



When these functions are misaligned — even slightly — risk management effectiveness deteriorates.

The issue is not absence of capability. It is the quality of integration.

The Three-part System

Effective ML/TF/PF risk management sits within a three-part system

GOVERNANCE

- Sets direction and risk appetite
- Provides oversight
- Holds accountability

MANAGEMENT

- Implements controls
- Allocates resources
- Executes strategy

COMPLIANCE

- Interprets regulatory expectations
- Monitors effectiveness
- Advises and challenges

Key message: No single function "owns" effectiveness — it is produced through interaction.

Compliance As Interpreter & Enabler

Compliance is often misunderstood as only a monitoring function

In practice, it plays a broader role:

- Interprets regulatory expectations
- Educates leadership on emerging risks
- Translates technical requirements into governance language
- Challenges assumptions and practices
- Advises on control effectiveness
- Provides assurance to governance structures

Critical point: Accountability sits with governance — but understanding is often enabled by compliance.

From Understanding To Alignment

A key challenge in ML/TF/PF risk management is not lack of accountability.

It is lack of alignment between:

- Control effectiveness
- Risk appetite
- Business strategy
- Regulatory expectation

Key message: Effective risk management depends on alignment, not isolation of roles. When alignment breaks down, escalation becomes reactive rather than preventive.

Anchoring Into The Regulatory Framework

FICA Sections 42 and 42A

Require accountable institutions to:

- Identify ML/TF/PF risks
- Assess and monitor risks
- Mitigate risks through an RMCP

GN 7A reinforces that:

- Governance structures must approve and oversee the RMCP
- Accountability rests with the institution
- Effectiveness must be demonstrated, not assumed

Financial Intelligence Centre

GUIDANCE NOTE

REVISED GUIDANCE NOTE 7A

Key interpretation: Regulation formalises what effective organisations should already be doing collaboratively.

Governance Vs Compliance (Clear Distinction)

Key distinction:

GOVERNANCE

Governance decides what acceptable risk looks like.

- Direction
- Oversight
- Accountability
- Risk appetite setting

COMPLIANCE

Compliance assesses whether reality matches that expectation.

- Interpretation
- Monitoring
- Advisory support
- Challenge and assurance

Where Governance, Management, and Compliance Intersect

These functions do not operate independently, but continually intersect

Key message:

Risk management effectiveness is determined at the intersection, not within silos.

This intersection is where compliance culture becomes visible in practice.

How Compliance Builds Governance Buy-in

Governance structures are typically focused on strategy, risk, sustainability, reputation, and accountability. Whereas compliance often reports activity metrics, policy updates, and monitoring statistics.

Effective compliance functions bridge this gap by translating information into governance relevance:

- What are our most material risks?
- Where are we exposed?
- Are controls effective in practice?
- What decisions require Board attention?

And this is our new manager in charge of compliance.

"He's in compliance ... but don't think he won't bite."

Key insight: Governance engagement increases when compliance information becomes decision-relevant.

Compliance Culture: The Connective Tissue

Compliance culture is not policy adherence or training completion. It is reflected in behaviour:

1. Escalation decisions
2. Responsiveness to issues
3. Leadership reinforcement
4. Tolerance for control weaknesses
5. Willingness to challenge decisions

"Culture eats strategy for breakfast."

— Peter Drucker (commonly attributed)

Key message: Culture determines whether governance intent becomes operational reality

From Reporting To Governance Intelligence

TRADITIONAL REPORTING

"98% AML training completion achieved."

Key distinction:
Reporting describes activity

GOVERNANCE-RELEVANT INSIGHT

"The highest-risk business unit shows the lowest AML training effectiveness."

Key distinction:
Governance intelligence highlights risk

Key message: Boards engage when information supports decisions, not when it describes activity.

What Effective Governance Looks Like

Effective governance does not mean operational involvement.
Nor does it mean passive approval.

Effective governance means:

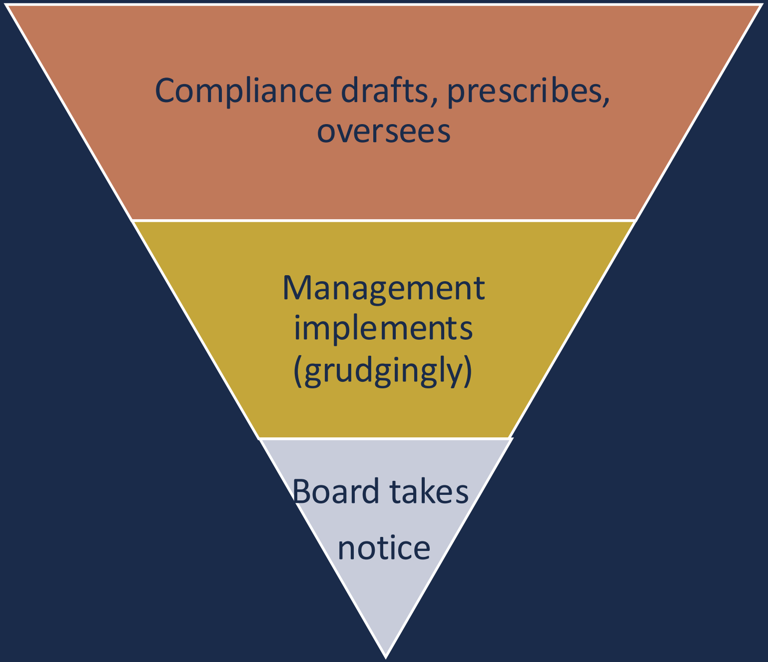
- Challenging assumptions
- Understanding risk
- Supporting independent oversight
- Asking informed questions
- Holding management accountable

The objective is informed oversight, not operational intervention.

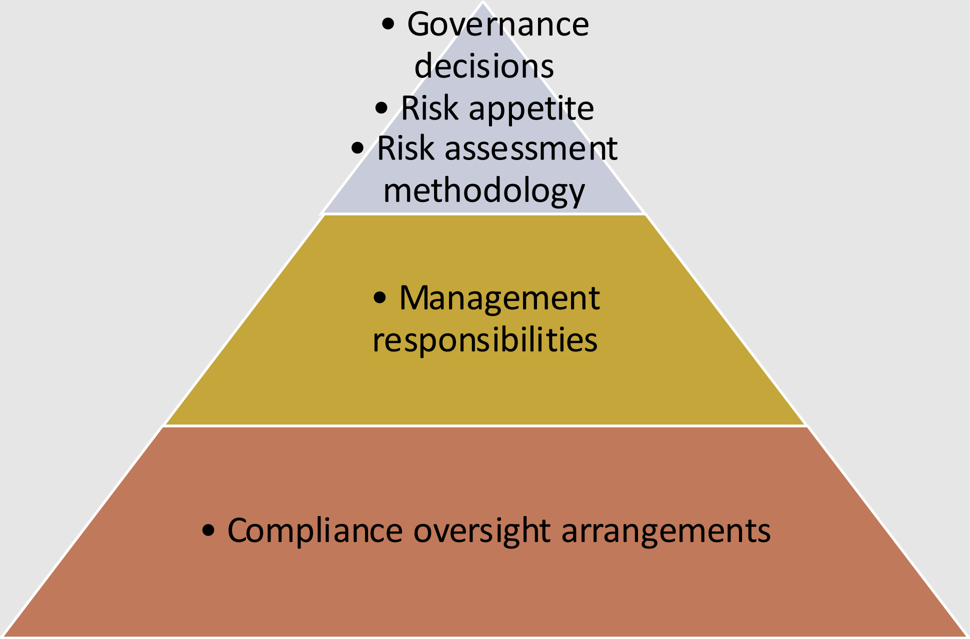
The RMCP as a Governance Document

The RMCP belongs to the institution. Governance structures must own it accordingly.

Traditionally, the RMCP has been viewed as a compliance document.



GN 7A requires a different perspective.



From Principles To Practice:

What Happens When The System Is Stressed?

The true test of governance is not how organisations operate when risks are low and controls are functioning.

The true test is how they respond when:

- Governance structures are required to challenge management assumptions
- Risks escalate
- Compliance concerns are raised
- Commercial pressures emerge
- Difficult decisions need to be taken

From Principles To Practice:

What Happens When The System Is Stressed?

The following examples illustrate four recurring patterns observed across institutions globally.

Importantly, these examples should not be viewed as governance failures or compliance failures, but rather, they demonstrate what can happen when the relationship between governance, management and compliance becomes misaligned.

As we consider each scenario, the question is not: *"Who was responsible?"*

The more useful question is: *"What can we learn about the interaction between governance, management, and compliance?"*

SCENARIO 1

When Information Does Not Become Action

Case Study:

Danske Bank

— the difference between awareness and action

Scenario 1: Danske Bank

Why is governance at the heart of this scandal?

Because anti-money laundering protocols begin at the top levels of a business.

- Its board and the executive team failed to give proper oversight.
- If senior leaders didn't facilitate money laundering themselves, they ignored red flags showing that others were doing so
- As a result of internal audits, information from regulators, and an internal whistleblower, Danske Bank knew that some customers were engaged in highly suspicious and potentially criminal transactions.
- Danske Bank also knew that some of its subsidiaries' anti-money laundering programs and procedures did not meet Danske Bank's global standards.

But they did nothing

Scenario 1: Danske Bank

In financial institutions, boards and executive teams have a crucial duty to ensure sufficient anti-money laundering (AML) controls.

As a result, the CEO and the Chairman of the Board of Directors stepped down

LESSONS

- Escalation alone does not manage risk
- Action and inaction bring similar consequences
- Effective governance requires challenge, prioritisation and action
- Foster a culture of accountability: Make compliance everyone's responsibility, from front-line staff to leadership

SCENARIO 2

When Commercial Objectives And Risk Management Become Misaligned

Case Study:

HSBC

BBC

HSBC to pay $1.9bn in US money laundering penalties

11 December 2012

Scenario 2: HSBC

Every institution experiences tension between growth objectives and risk management requirements.

The question is not whether this tension exists. The question is how it is managed.

Rapid growth but did not invest adequately in AML systems, staffing, or governance.

Combination of high volume growth, legacy systems and weak oversight = environment where serious money laundering and sanctions risks were not effectively managed.

Scenario 2: HSBC

Every institution experiences tension between growth objectives and risk management requirements.

The question is not whether this tension exists. The question is how it is managed.

HSBC

Inadequate AML Programme:

HSBC operated with understaffed compliance teams, outdated systems, and significant alert backlogs.

HSBC's compliance issues stemmed from cost-cutting and restructuring that weakened its oversight mechanisms.

Scenario 2: HSBC

HSBC’s global structure made it difficult to enforce consistent AML standards across regions, and group-level oversight did not sufficiently challenge local risk-taking and control gaps.

Scenario 2: HSBC

Red Flags That Should Have Triggered Stronger Action:

- Long-standing deficiencies in AML systems and staffing levels in key locations.
- Repeated findings from regulators and internal audits highlighting weak controls.
- **The source of these failures was a corporate culture that prioritized profits over ethical conduct**

Regulatory & Legal Consequences:

In total monetary penalties and forfeiture of approximately **$1.9 billion.**

Significant **reputational damage** and heightened supervisory expectations globally.

Scenario 2: HSBC

The HSBC enforcement action demonstrated the consequences of allowing business objectives and risk management realities to diverge.

Effective governance ensures that strategic ambitions remain aligned to risk appetite and control effectiveness.

SCENARIO 3

When Independence And Collaboration Fall Out Of Balance

Case Study:

Westpac

- a $1.3Bn fine

Scenario 3: Westpac

The Governance Breakdown: When Senior Management Loses Control

- **“Indifference”** of senior management towards compliance
- **The bank was warned** about its systemic failures but was either slow to act or did nothing about it.
- **Inadequate Oversight:** Westpac flatly admitted it “did not have a consistently clear understanding and appreciation” of its anti-money laundering and counter-terrorism financing obligations.
- **Poor Risk Assessment:** Westpac “adopted an ad hoc approach to ML/TF risk management and compliance”.
- **Delayed Response:** Even after becoming aware of compliance breaches, the bank failed to treat remediation as a priority, allowing problems to compound over time.

Scenario 2: HSBC

The Leadership Exodus: Accountability at the Top

The scandal ultimately cost Westpac its senior leadership. CEO and Board Chairman both resigned as the full extent of the compliance failures became apparent.

This demonstrates that in today's regulatory environment, compliance failures aren't just operational issues—they're career-ending events for senior executives.

Risk Management and Governance Lessons from the Westpac Case :

Do you have clear accountability for compliance at the senior management level?

Compliance can't be delegated to operational staff without senior oversight and accountability.

SCENARIO 4

What Effective Governance Looks Like in Practice

MATURE AML PROGRAMMES

Culture

- Open escalation channels.
- No penalty for raising concerns
- Consistent leadership messaging
- Shared understanding of ML/TF/PF risks

Governance

- Board-approved risk appetite
- Challenge of risk assessments and RMCP assumptions
- Focus on effectiveness rather than activity metrics

Management

- Ownership of remediation actions
- Alignment between business strategy and risk appetite
- Adequate resource allocation

Compliance

- Direct access to governance structures
- Regular AML/CFT education for Board members
- Independence combined with commercial understanding.
- Reporting focused on risk insights rather than statistics

Compliance Officer identifies an emerging sanctions-risk exposure linked to a new product offering.

Escalated to management

Management evaluates the operational impact and resource implications

Compliance explains the regulatory exposure and potential consequences

Board Risk Committee challenges assumptions, seeks additional information and assesses whether the exposure falls within the institution's risk appetite.

A decision is made to proceed only after additional controls are implemented

Six months later the controls are independently reviewed and reported back to governance structures.

"Whose success was this?"

The answer is:

Not Compliance. Not Management. Not the Board.

It was the success of a governance system functioning as intended.

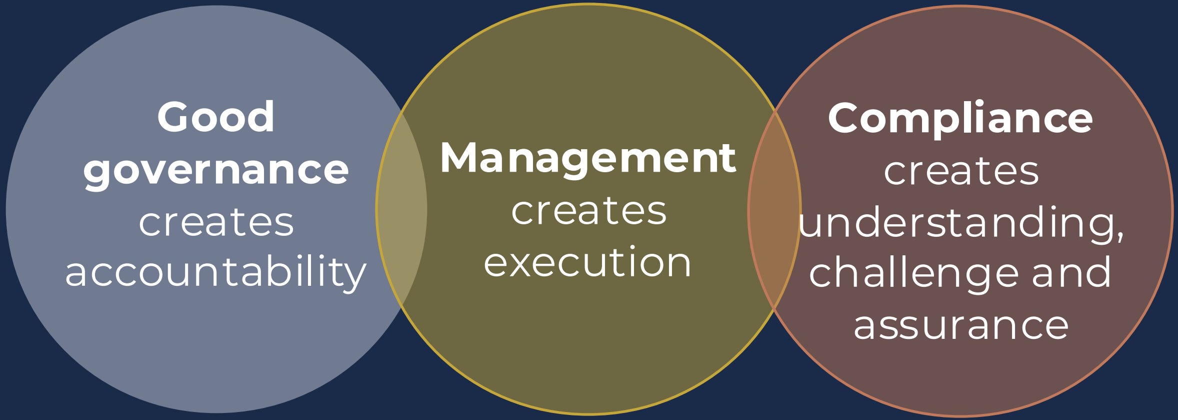
A Shared Responsibility

The message of GN 7A is not that compliance becomes less important or more important.

The message is that effective ML/TF/PF risk management depends upon **governance, management and compliance working together in a manner that promotes transparency, accountability and informed decision-making.**

A Shared Responsibility

Accountability may sit with governance structures, but effective accountability depends on shared understanding — and that is often where compliance plays its most important role.



Culture connects all three

“The tone at the top is important, but it is the mood in the middle that drives behaviour.”

— Paul Sobel,
former Chairman of COSO

Accountability may sit with governance structures.
But **effective accountability begins with understanding**, and understanding is often where compliance makes its greatest contribution.

GATEKEEPING CONSULTING