How a Well-defined Target Operating Model Can Enhance AML Risk Management in General, and Internal Audit in Particular

ACAMS (Audit) White Paper

Marcus Keisers, CIA, CAMS

EXPOSEE

As an anti-money laundering (AML) auditor, you should not only make sure to audit the right processes and controls, but you should also be able to demonstrate completeness and consistency in identification and coverage of these elements of a risk management framework. In this context, a well-defined Target Operating Model (TOM) is not only a cornerstone for AML risk management, but also an effective method to enhance the internal audit function.

This paper discusses the considerations in developing a TOM across the organization and how this can be translated into a dedicated TOM for internal auditors in order to comprehensibly and effectively manage AML risk.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Global regulatory expectations, including the Federal Reserve[1] (the Fed), require a firm-wide approach across business lines, legal entities, and jurisdictions for AML risk management. Respective cease and desist orders show zero tolerance for any deficiencies, and once they have been identified, it is not only about fixing certain parts of the compliance program. Rather, enhancement of the whole risk management framework is required. Due to the complexity and the different stakeholders within large organizations, the challenge is to create ownership for processes and controls in order to make sure that the necessary resources are dedicated to fully implement an effective compliance program.

In order to meet regulatory expectations, risk management should start at the governance level, including well-defined organizational responsibilities, typically referred to as the three lines of defense (3LoD).[2] Based on this 3LoD principle and a clear definition of AML risk (and further major risk types), a TOM can be derived that provides ownership of processes and controls along the compliance/AML risk management process. This raises stakeholders' awareness of regulatory requirements and respective changes across the whole organization, which enables the organization to identify and dedicate the necessary resources responsible for transforming regulatory requirements into consistent policies, procedures, and controls. In this context, the first line of defense (1st Line) is the so-called "risk owner" responsible for implementing processes and controls. The second line of defense (2nd Line) is the "standard setter and monitor" who creates standards in the form of policies and monitors their compliance.

The task of the internal audit function as the third line of defense is the independent examination of the processes and safety precautions of the bank, and therefore the assessment of the activities of the first and 2nd Line. In order to do that efficiently, the internal auditor should align the organizational structure, audit universe, audit work programs and procedures, as well as audit reports and management information with the elements and organizational responsibilities of the overarching TOM. This enables the internal audit function to demonstrate completeness and consistency in coverage of all elements of the compliance/AML risk management program across all lines of defense. Furthermore, results can be presented in a well-structured way to provide vital input on the effectiveness and status of the AML risk management framework for the 1st and 2nd Lines of defense.

[1] See Supervisory Letter SR08-8, "Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles."
[2] BCBS 328 - Corporate governance principles for banks, paragraph 38.

II. Expectation on Compliance Risk Management and respective challenges

a) Regulatory Expectation

According to the Fed,[3] large banking organizations operating with multiple business lines and legal entities in different jurisdictions require a firm-wide approach for compliance risk management, especially in the area of AML. A respective risk management framework for identifying, assessing, controlling, measuring, monitoring, and reporting compliance risk across the organization should be formalized and documented in a compliance program consisting of respective policies, procedures, and controls.

Based on a review of respective cease and desist orders in recent years, the following issues and recommendations have been identified with respect to the compliance risk management frameworks/programs[4]:

- Ensure global compliance with laws and regulations (November 19, 2018, Société Générale S.A.)
- No effective firm-wide risk management framework that covered all key risks (February 2, 2018, Wells Fargo)
- Implement an effective compliance risk management framework (August 3, 2016, The Goldman Sachs Group, Inc.)
- Implement an enhanced program to ensure global compliance with U.S. sanctions and AML laws (March 12, 2015, Commerzbank AG)
- Implement a program to ensure global compliance with U.S. sanctions laws (June 30, 2014, BNP Paribas S.A.)
- Inadequate risk management and compliance program (May 19, 2014, Credit Suisse AG)

The identified issues and related requirements show the holistic approach the Fed is taking for large organizations. It is not sufficient to only address certain parts of a compliance program, but rather, enhancement of the whole risk management framework is required by almost all cease and desist orders.

b) Challenges to meet regulatory expectation

Challenges to implement a firm-wide compliance risk management program arise from the fact that business activities often span around the globe and across jurisdictions. Different regulatory requirements need to be taken into consideration and often cause a multinational impact. These requirements need to be analyzed and transformed into consistent policies, procedures, and controls. In order to do that effectively, various stakeholders within the organization need to cooperate. However,

[3] See Supervisory Letter SR08-8, "Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles."
[4] www.federalreserve.gov - for further details see also "References."

if there is no ownership of these topics, regulatory requirements and respective changes might go undetected. Even if requirements are identified, risk management might be hampered due to unclear roles and responsibilities for respective implementation.

The challenge for the internal auditor is to not only to identify and audit the important aspects, but to traceably cover all elements of the risk management framework and include all stakeholders and their interfaces with no blind spots. In this context, the aforementioned challenges regarding unclear roles and responsibilities are also immanent to the internal audit function. It needs to be clear who is auditing what aspects of the AML risk management framework to ensure consistent coverage.

III. Enhancing Compliance Risk Management by applying a TOM

a) Three lines of defense

According to BCBS 328 "Corporate governance principles for banks" (BCBS 328), *a risk governance framework should include well-defined organizational responsibilities for risk management, typically referred to as the three lines of defense.*[5]

The 3LoD principle contains the following elements in accordance with BCBS 328:

- The **first line of defense (1st Line)** is the so-called "**risk owner**." It is that place at which the risk comes into the bank. The 1st Line is therefore responsible for the risk identification, evaluating, mitigating, or preventing risk in the daily business. For these purposes, the **1st Line implements processes and controls** and defines a business risk strategy, including a specific risk appetite statement for the area of responsibility.
- The **second line of defense (2nd Line)** is the "**standard setter and monitor**" for risks that have arrived in the bank. Its task lies in the control, limitation, and monitoring of risks. For this purpose, the **2nd Line creates standards in the form of policies and monitors their compliance**. It decides the overall risk appetite of the bank for the respective risk type and evaluates/reports on risks. It examines the controls of the 1st Line through downstream control activities. In addition, the 2nd Line escalates if necessary.
- The **third line of defense (3rd Line)** is the "**internal audit**." Its task is the independent examination of the processes and safety precautions of the bank, and therefore also the **assessment of the activities of the 1st and 2nd Line**.

However, organizational units can move across the lines of defense depending on the risk type. For example, an employee of the compliance function or internal audit becomes the 1LoD in preventing cyber risk when choosing its user passwords and making sure nobody else has access to it. Therefore, different parts of the organization are responsible for managing different risk types, especially from a 2nd Line perspective, and the risk management framework should be built on a clear

[5] BCBS 328 - Corporate governance principles for banks, paragraph 38.

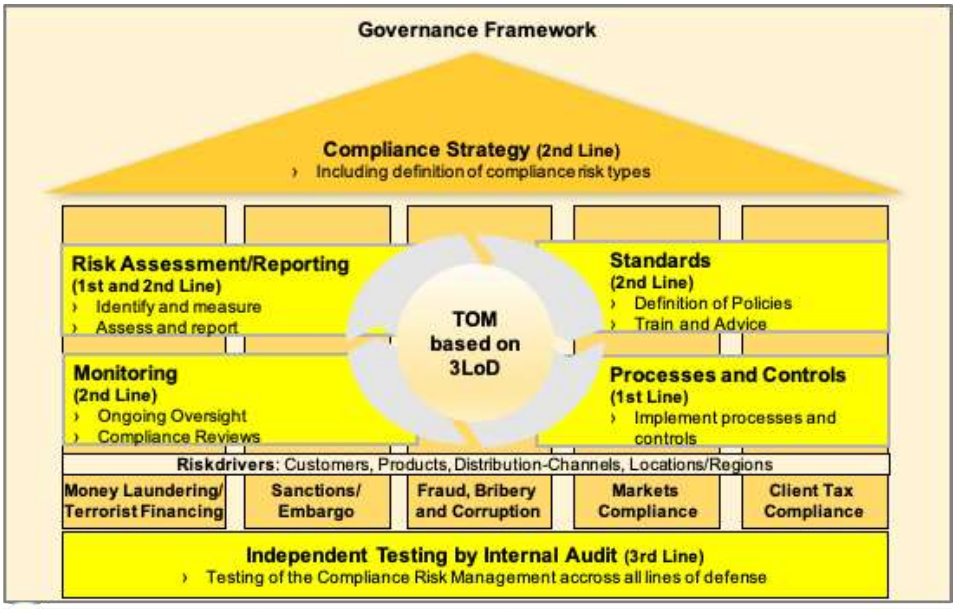
definition for each of the major risk types to ensure consistent coverage with no gaps. Interfaces and overlaps between risk types (e.g., between operational risk and AML risk) should be defined, as well.

Generally speaking, compliance risk arises from being non-compliant with laws and regulations as well as applicable rules and standards.[6] However, further clarification of compliance risk and definition of specific risk types, like AML, helps to further clarify roles and responsibilities according to the 3LoD. In addition, the importance of AML risk, which, unlike other risks, is not only quantitative in nature but carries a lot of qualitative aspects, can also be emphasized. In this context, it is normally no economical approach you can take to manage AML risk (like for credit risk when accepting a certain probability of default), but rather, a zero-tolerance approach. All these aspects should be taken into consideration when defining AML risk.

b) Transformation into a TOM

Having defined AML risk and further major risk types as a pre-condition, the 3LoD-principle provides activity-based guidance, which can be depicted and further transformed into a TOM to apply a consistent approach to ensure comprehensive, firm-wide compliance/AML risk management. This delineation of roles and responsibilities assigns clear ownership of topics along the risk management process (see diagram below). As a result, stakeholders' awareness for regulatory requirements will be raised across the whole organization. This will also facilitate the assessment of change in regulations and respective impact analysis. Based on that, the organization will be enabled to identify and dedicate the necessary resources that are responsible for transforming regulatory requirements into consistent policies, procedures, and controls.

[6] BCBS 113 - Compliance and the compliance function in banks.

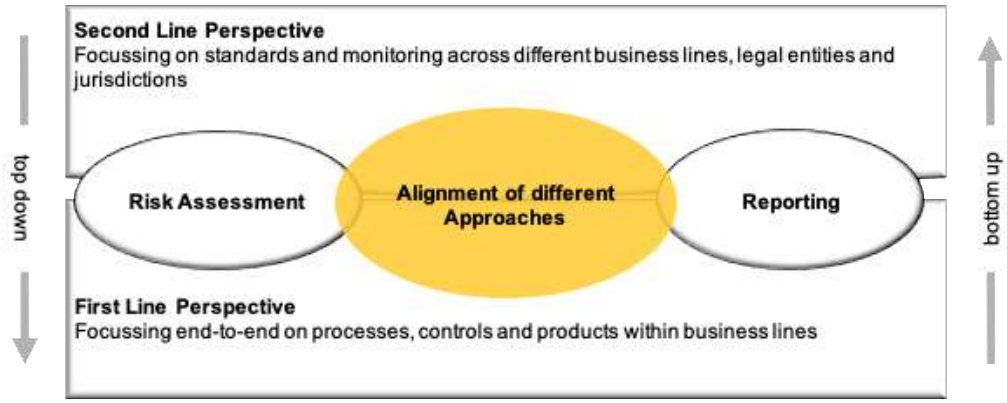


3LoD-principle can be transformed into a TOM to assign clear ownership of topics along the AML risk management framework

IV. Enhancing Internal Audit by applying a dedicated TOM

a) Different Audit Approaches

Based on the organizational responsibilities, according to the TOM, there are two different approaches or perspectives (i.e., either the 1LoD perspective and/or 2LoD perspective) to audit the AML risk management framework. Either you can start on product or process level (i.e., bottom-up), or you can choose a top-down approach starting on the governance level with respective standards. However, both approaches need to be aligned to comprehensively cover all elements of the AML risk management framework (i.e. identifying, assessing, controlling, measuring, monitoring, and reporting). Also, the interaction between 1LoD and 2LoD should be regularly addressed in respective audits to ensure that there are no blind spots or uncertainties regarding responsibilities in the overlapping areas, like assessing and reporting AML risk consistently.



Demonstrate complete coverage of the AML risk management framework by applying a consistent approach along the Target Operating Model

b) Dimensions of a dedicated TOM for Internal Audit

In order to align the different approaches and to ensure full coverage of the AML risk management framework, defined by the overarching TOM, a dedicated TOM for internal audits should be implemented covering all of the following dimensions of an internal audit function:

- Audit organization
- Audit universe
- Audit Work Programs (AWP)
- Audit planning process
- Audit reports
- Management information system (MIS) and key performance indicators (KPI)

a. Audit Organization

Audit divisions responsible for covering 2nd Line functions, including compliance, should be identified and clearly stated in the business objectives of the audit function. Further, it should be stated which audit divisions are responsible for covering the business lines and support functions. In the end, all major risk types and respective 2LoD, as well as all business lines and support functions, should be reflected in the business objectives to assign clear ownership within internal audits.

b. Audit Universe

In order to build a consistent and complete audit universe, the different perspectives of the TOM should be matched to the audit objects and included in the respective descriptions. From that, it should be clear where the standards and monitoring aspects are covered and how they align to products, processes, and controls. All business lines, legal entities, and jurisdictions should be included and aligned, as well. In the end, it must be traceably documented how the Audit Objects (AO) consistently cover 1LOD and 2LOD perspective. Most likely, there are AO for products (e.g., trade finance) and for processes (e.g., KYC and CTO) covering 1LoD-perspective end-to-end within a business line. Besides that, there are AO that cover elements of the TOM from a 2LOD perspective across business lines, entities, and jurisdictions (e.g., AML risk assessment, transaction monitoring, compliance framework).

AO for AML risk management, focusing mainly on the 1st Line perspective, may for example include:

- KYC and CTO procedures
- Client life cycle management
- Certain products (e.g., trade finance) with AML risk exposure
- Payment and account services

AO for AML risk management focusing on the 2nd Line perspective may, for example, include:

- Compliance framework/strategy
- Risk assessment methodology
- Training program
- Transaction monitoring

c. Audit Work Programs (AWP)

AWP should be structured along the different activities (i.e., risk assessment, reporting, standards, training, processes, controls, and monitoring) and organizational responsibilities according to the TOM. By doing that, you can clearly reference whether you cover 1st or 2nd Line perspective during fieldwork. Furthermore, you ensure consistent coverage across business lines, products, and jurisdictions.

Please find on the next page an example of an AWP for a compliance and client life cycle management (CLM) program that has been structured this way. For the purpose of simplification, and to provide a good overview, it has not been further specified how to perform respective tests of design and effectiveness of operation.

Topic	**Activity** (acc. to TOM)	**LoD** (acc. to TOM)	Testing **Objective and Scope**
Compliance Organization	Governance Framework	2nd Line	Appropriate definition of roles & responsibilities, including designation of and responsibilities of AML officer, as well as appropriateness of the organizational structure of group compliance
CLM Organization	Governance Framework	1st Line	Organizational structure (including segregation of duties, reporting lines) and definition of roles & responsibilities for CLM process
Overall AML Committees	Governance Framework	2nd Line	Appropriateness of AML committee structure to facilitate cross-departmental/cross-locational information exchange and decision taking in the compliance function
CLM Committees	Governance Framework	1st Line	Appropriateness of committee structure to facilitate cross-departmental/cross-locational information exchange and decision taking in CLM
Staffing	Governance Framework	2nd Line	Appropriate staffing, fluctuation, and dependency of key staff in the compliance function
Staffing	Governance Framework	1st Line	Appropriate staffing, fluctuation, and dependency of key staff involved in CLM (front office and support functions)
Legal and Regulatory Research	Standards	2nd Line	Processes and implemented controls defined to identify legal and regulatory requirements/changes
Global Minimum Standards	Standards	2nd Line	Implementation of group-wide compliance standards covering aspects like compliance risk assessment, trainings, KYC, CLM, AML monitoring, etc.
AML Policies & Procedures	Standards	2nd Line	Adequacy of overall AML-related written framework including completeness (with global standards, coverage of local regulatory requirements, and coverage of specific risks; i.e., correspondent banking/trade finance) and consistency (with global standards and across business lines)
CLM Procedures	Processes & Controls	1st Line	Adequacy and appropriateness of processes and controls to identify and verify customers, including customer risk rating, screening of customer base, and periodic KYC reviews
Risk Assessment Methodology	Risk Assessment	2nd Line	Appropriateness of the methodology and approach for the group-wide AML risk assessment
Risk Assessment	Risk Assessment	1st Line	Application of the risk assessment methodology in the business segments to identify, assess, measure, and report AML risks
Compliance Reviews	Monitoring	2nd Line	Adequateness of AML-related compliance reviews
Transaction Monitoring	Monitoring	2nd Line	Evaluation of the adequacy of the transaction monitoring program including alert/case processing
AML Training	Train and Advice	2nd line	Up-to-datedness, completeness, and accuracy of the AML training program
Compliance Reporting	Reporting	2nd Line	Appropriate intra-corporate communication (within location and with head office) as well as external communication with supervisory and regulatory authorities
CLM Reporting	Reporting	1st Line	Appropriateness of the intra-corporate communication (including effective interfaces to other parties involved) and reporting metrics to ensure an adequate handling of CLM tasks

d. Audit Planning

When planning audits, the following questions need to be answered beforehand to ensure that all relevant TOM aspects are recognized and traceably covered:

- What risks and respective risk types are relevant and will be in scope?
- What are the risk drivers?
- What business units, entities, and jurisdictions are relevant?
- What parts of the risk management framework will be in focus (i.e., 1st Line and/or 2nd Line perspective)?
- Who are the responsible stakeholders in the 1st and/or 2nd Line?

Based on that, the following needs to be decided:

- The resources (audit departments) that will take part in the audit
- The audit objects that are covered
- The parts of the AWP that are in scope
- The interaction/alignment between 1st and 2nd Line perspective

e. Audit Reports

The content of audit reports and the way they are structured should also reflect the elements of the TOM. It should be clearly marked which elements have been covered, and the outcomes. This ensures traceability of completeness and comparability of results. Furthermore, this provides the possibility to consolidate results in a respective management reporting.

f. Management Information System (MIS) and Key Performance Indicators (KPI)

The different stakeholders of an MIS are not only located within the internal audit function, but also senior management of the 1st and 2nd Line of defense. In order to assess the effectiveness of the TOM, management reporting for all those stakeholders should reflect, on a consolidated basis, which elements have been covered as well as the outcome. Due to the consistency with audit reports, audit objects, and AWP, this should also allow for a breakdown of results when deemed necessary. Hence, the overall advantage is that results can be consolidated and be broken down again to products, business lines, and entities as needed. The advantage for internal auditors is the ability to demonstrate which elements were covered, and the results. Gaps can be identified by mapping the overall TOM elements to the TOM elements covered by audit.

KPI with respect to AML risk management may include, for example:

- Total amount of AO covering 1st Line perspective versus amount of respective AO audited in the last 12 months, including results
- Total amount of AO covering 2nd Line perspective versus amount of respective AO audited in the last 12 months, including results
- Aggregated results for certain products and processes in the 1LoD
- Aggregated results for standards and monitoring in the 2LoD

- Total number of AWP content regarding AML risk management, including respective activities according to TOM (i.e., risk assessment, reporting, standards, training, processes, controls, monitoring) versus amount covered, including results (i.e., overall and per element)
- AWP content covered during the last 12 months, including respective organizational responsibilities and results per organizational unit (i.e., aggregated and per element)

V. Conclusion

a) Implementing a TOM will enhance AML Risk Management

Based on the 3LoD principle, a TOM can be derived that provides a consistent framework to ensure a comprehensive and bank-wide, as well as structured and holistic, approach to managing AML risk. This will foster ownership of processes and controls across all stakeholders, enabling the organization to:

- raise stakeholder awareness for regulatory requirements;
- facilitate the assessment of change in regulations and the respective impact on the organization;
- identify and dedicate necessary resources;
- demonstrate completeness and consistency in coverage of requirements.

b) Implementing a dedicated TOM for Internal Audit will further enhance AML Risk Management

Internal audit as the 3rd Line of defense should further translate the overarching TOM into a dedicated TOM for internal auditors. Reflecting the TOM in its own setup across all dimensions will enable the internal audit function to:

- identify and audit the right processes and controls with no blind spots or gaps;
- demonstrate completeness and consistency in coverage of requirements;
- inform all stakeholders adequately about the status and effectiveness of the AML risk management framework/program.

ACRONYMS AND ABBREVIATIONS

AML	Anti-money laundering
AO	Audit Object
AWP	Audit work program
BCBS	Basel Committee on Banking Supervision
CLM	Client Lifecycle Management
Fed	Federal Reserve Bank
CTO	Client take-on
KPI	Key performance indicators
KYC	Know Your Customer
MIS	Management information system
TOM	Target operating Model
3LoD	Three lines of defense
1st Line	First line of defense
1LoD	See “1st Line”
2nd Line	Second line of defense
2LoD	See “2nd Line”
3rd Line	Third line of defense
3LoD	See “3rd Line”

REFERENCES

- Basel Committee on Banking Supervisions - Compliance and the compliance function in banks (BCBS 113).
- Basel Committee on Banking Supervisions (BCBS) - Guidance on Corporate governance principles for banks (BCBS 328).
- Cease and Desist Orders. www.federalreserve.gov:
  - November 19, 2018 Société Générale S.A.:
    The Federal Reserve's order requires Société Générale to implement an enhanced program to ensure global compliance with U.S. sanctions administered by the U.S. Department of Treasury's Office of Foreign Assets Control.
  - February 2, 2018 Wells Fargo:
    In recent years, Wells Fargo pursued a business strategy that prioritized its overall growth without ensuring appropriate management of all key risks. The firm did not have an effective firm-wide risk management framework in place that covered all key risks. This prevented the proper escalation of serious compliance breakdowns to the board of directors.
  - May 13, 2017 Deutsche Bank AG:
    The Board identified failures by Deutsche Bank's U.S. banking operations to maintain an effective program to comply with the Bank Secrecy Act and anti-money laundering laws.
  - August 3, 2016 The Goldman Sachs Group, Inc.:
    The board of directors of Goldman Sachs must ensure that its senior management implements an effective compliance risk management framework and that potential compliance risk failures are appropriately brought to the attention of senior managers and addressed immediately.
  - March 12, 2015 Commerzbank AG:
    The order requires Commerzbank, including its branch in New York, to implement an enhanced program to ensure global compliance with U.S. sanctions and anti-money laundering laws.
  - June 30, 2014 BNP Paribas S.A.:
    The cease and desist order requires BNP Paribas to implement a program to ensure global compliance with U.S. sanctions laws.
  - May 19, 2014 Credit Suisse AG:
    The order requires Credit Suisse to complete its ongoing efforts to implement programs and policies to ensure that Credit Suisse conducts its operations in the United States and worldwide in full compliance with U.S. banking laws and the contemporaneous orders of the Department of Justice and the New York State Department of Financial Services.
- Supervisory Letter SR08-8, “Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles.”