BUILDING YOUR COMPLIANCE RISK ASSESSMENT AND THE ROLE OF CONTROL TESTING

Uche Iwuchukwu
EMEA Head of Compliance Testing,
Morgan Stanley

Wiecher Mandemaker
Head of Testing and Monitoring Services,
Nordea

TODAY'S TOPICS

Considerations for developing and running an effective solution

- Why have a Compliance Risk Assessment?
- Risk Identification vs Risk Assessment
- Risk Assessment Components
- The role of Control Testing

RISK IDENTIFICATION VS RISK ASSESSMENT

Identify the applicable requirements

Regulations (consider all levels; local, regional, organisational).

Charters, commitments etc. that the organisation has agreed to follow.

Identify the risks that could arise

What will cause a risk to materialise (activities, customers, geography, processes).

Assess the effect or impact of those risks

The focus of today's presentation!

RISK ASSESSMENT

For purpose of this presentation:

Risk Assessment:
The (independent) evaluation of risk exposure through the assessment of risks and associated controls that are subject to oversight by the compliance function…

… performed by the compliance function and expressed against a fixed set of criteria or values for comparison.

Supports prioritisation or risk based approach to compliance activities

Provides an independent view to benchmark other assessments in the organisation

Supports a consistent approach to reporting on compliance risk

WHY HAVE A COMPLIANCE RISK ASSESSMENT?

REGULATORY FOUNDATION

Identification, measurement and assessment of compliance risk
The compliance function should, on a pro-active basis, identify, document and assess the compliance risks associated with the bank's business activities…….

Compliance programme:
The responsibilities of the compliance function should be carried out under a compliance programme that sets out its planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessment, compliance testing, and educating staff on compliance matters. The compliance programme should be risk based and subject to oversight by the head of compliance to ensure appropriate coverage across businesses and co-ordination among risk management functions.

From: *Basel Committee on Banking Supervision (BIS) - Compliance and the compliance function in banks*

CONSIDER..

Before setting out on designing your risk assessment approach, consider what you will use the output for:

- Developing your Compliance Plan
  - Training
  - Advisory Activities
  - Testing/Monitoring/Assurance
- Reporting to the First Line of Defence
- Reporting to the Board / Board committees
- Assessing Risk Appetite exposure
- Other?

RISK ASSESSMENT COMPONENTS

BUILDING BLOCKS

No Financial Institution is the same, so any risk assessment needs to be designed to fit the needs of your Compliance programme.

There are key components and considerations that we will review today, as well as ranges of options that can be considered, such as:

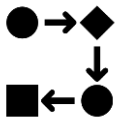
- ✓ Risk Categorisation/Taxonomy
- ✓ Organisational units
- ✓ Risk drivers / regulatory obligations
- ✓ Assessment Grids
- ✓ Alignment to other risk processes in the organisation
- ✓ Resources / Sources of information
- ✓ Cycle / Frequency of Assessment

CATEGORISATION / TAXONOMY

Consider how your organisation measures and reports compliance risk information

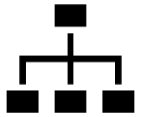
Regulatory Obligations

- AML Directive
- MiFiD



Business Activities / Operational Processes

- KYC for Large Corporates and Institutions
- Data processing for retail customers in France

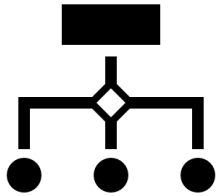


Existing Taxonomies or Categories in place

- Operational Risk Taxonomy
- Compliance Risk themes (e.g. Data Privacy, Conduct, Anti-Money Laundering, etc.)

ORGANISATIONAL UNITS

Determine at what level in the organisation you will assess and report your risk assessment result. This can range from very granular levels to consolidated levels.



Consider what is the lowest level of organisational unit that you will need to make the risk assessment meaningful and useable. This may also be influenced by regulatory requirements or expectations.

Individual Organisational Units
Sub business line level in a country (e.g. Fixed Income desk in Country X)

Aggregate Organisational Units
(e.g. Fixed Income in Europe)

It is often easier to aggregate than to disaggregate, so ensure that you obtain data at the lowest organisational level needed.

RISK DRIVERS / PROCESS INPUTS

✓ Risk Categorisation

✓ Organisational Units

Consider
Does the risk materialise/manifest itself through:

- Certain processes
- Certain activities
- Customer levels/types
- Geographies of operation
- Other?

At the beginning of the assessment process, consider describing for each risk category what the drivers are and whether/how they apply to the organisational units. This will support a consistent approach during the assessment.

ASSESSMENT GRIDS / DIMENSIONS

A typical approach consists of:

- Assessing the Inherent Risk
- Assessing the Control Environment
- Calculating the Residual Risk

Considerations – Inherent Risk
Is there an agreed measurement for Non-Financial Risk in your organisation (if yes, is it suitable for measuring Compliance Risk)
Is there an agreed gradation (e.g. red, amber green, assigned numerical measures) for expressing the severity of risk that is or can be used by the First, Second and Third for expressing risk.
Some organisations use scenario analysis to drive the inherent risk determination.
Using a direct expression of inherent risk based on professional judgement (e.g. the inherent risk is X), versus using an Impact and Probability Grid.

ASSESSMENT GRIDS / DIMENSIONS

A typical approach consists of:

- Assessing the Inherent Risk
- Assessing the Control Environment
- Calculating the residual risk

Considerations – Control Environment
How do controls get assessed rated by the First Line of Defence, Audit, Operational Risk).
Do you separately assess the control design dimension and operating effectiveness of the control or is there a single rating?
Is there an agreed measurement for Non-Financial Risk in your organisation (if yes, is it suitable for measuring Compliance Risk?)

We will cover the control aspect in more detail later in the presentation.

ASSESSMENT GRIDS / DIMENSIONS

A typical approach consists of:

- Assessing the Inherent Risk
- Assessing the Control Environment
- Calculating the residual risk

Considerations – Residual Risk
Consider a pre-defined formula or grid to combine the Inherent Risk and Control ratings.
Avoid overrides as much as possible to ensure a consistent application and comparable outcomes

ALIGNMENT TO OTHER RISK PROCESSES IN THE ORGANISATION

- Operational Risk Assessments
- Financial Crime Enterprise Wide Risk Assessments
- Audit Risk Assessments
- First Line Risk and Control Assessments
- Any other measurement of risks or controls

- What measurement scales are applied?
- What reporting scales are used
- Is there a need (or desire) to be aligned or is there sufficient drive to report independently.

RESOURCES / SOURCES OF INFORMATION

What are the data points available for you to assess the Risk Dimension and Control Dimension?

Compliance Testing, Monitoring, Assurance reports	Internal/External Audit reports	Issues and/or Incidents related to Compliance Risk	Proposed Legislation/ Regulation
Emerging regulatory focus areas	Reports on Regulatory Breaches	Business strategy information	Industry Trends

CYCLE / FREQUENCY OF ASSESSMENT

Annual Standalone Cycle / Annual Cycle with Periodic Update / Annual Cycle with Trigger Updates

What alignment (if any) is required to other processes?

- Are resources available, does the timing need to match other assessments in the organisation to be able to compare outputs?

What are the dependencies for data input?

- When will data sources be available
- How do you use the most current information

Output?

- What reporting needs to be generated?
- What processes does the risk assessment feed into (e.g. Annual Compliance Plan)

REPORTING

- Standalone vs Integrated reporting
  - Is the Risk Assessment an input for other processes (e.g. Annual Compliance Plan) or a standalone communication?
  - Who will use the risk assessment: Compliance, Risk Function, Senior Management, Board members, Others?

LEVERAGING CONTROL TESTING IN THE RISK ASSESSMENT

CONTROL TESTING

Connection to the Risk Assessment

- Well defined (key) controls should be able to substantially inform your control environment assessment.
- Some considerations:
  - Are they linked to the relevant regulatory risk areas?
  - Are they sufficient in organisational coverage?
  - Are the measuring / reporting scales connected.

INHERENT RISK DRIVERS VS CONTROL ENVIRONMENT DRIVERS

Inherent Risk

- Gradual moves – e.g. increasing regulatory expectations
- Major strategic developments – e.g. business expansion/contraction or significant external events

Control Environment

- Unexpected events (e.g. issues/incidents)
- Planned review activities (Compliance, Audit, Regulators)

Control Testing can be used for both control validation and gap detection.

CONTROL EVALUATION

Design and Control Effectiveness Assessments

Consider the frequency of control design effectiveness assessment.

- When starting control testing (initial).

- When the control has changed.

- Periodic (risk driven) refresh.

Once the design has been deemed (sufficiently) effective, then the focus should be on ongoing assessment of the operating effectives. This will deliver the meaningful input into the Risk Assessment.

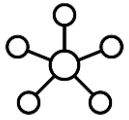
The ongoing assessments can (and typically should be) standardised to allow for comparison over time. Unless the key control has changed, a functioning operational effectiveness assessment should be repeatable.

There should not be a need to repeat the design assessment.

LINKING CONTROL TESTING BACK TO THE RISK ASSESSMENT

Timing and frequency

Ratings

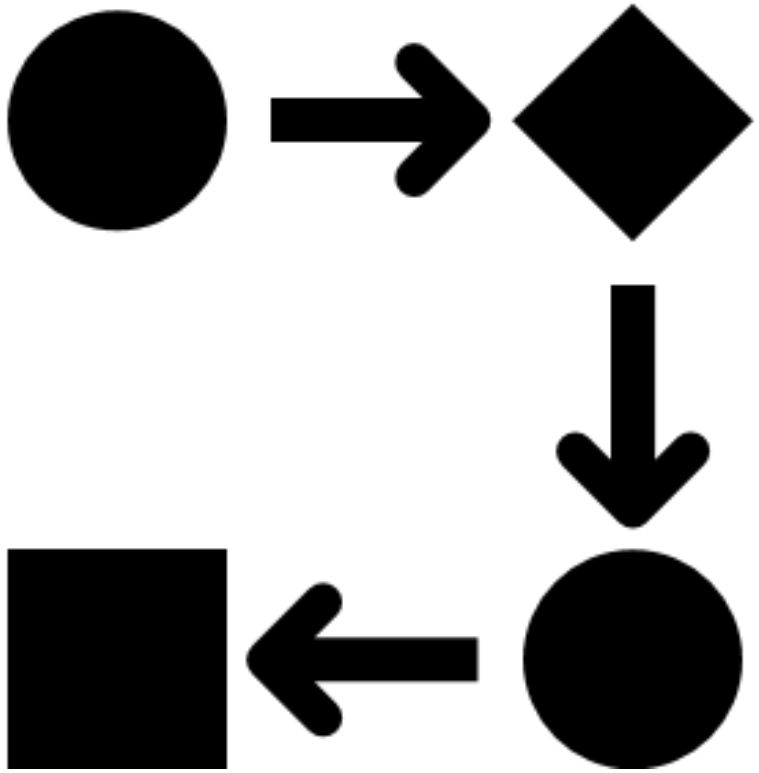


Assessing risk coverage

- Higher risk areas typically have more frequent control testing than lower risk areas.
- Does the testing align to the assessment cycle, does it drive a periodic update or both?
- Are the ratings for reporting control testing on the same scale as the control environment.
- Is there a minimum number of key controls that make up the control environment? Do they aggregate the same for all risks?
- It may be more relevant and expedient to review the appropriateness of (key) control coverage (i.e. are there sufficient controls all risks/areas in the risk assessment) separately from the control design and effectiveness assessment.

CONNECTING THE COMPONENTS

- With sufficient (key) control testing in place, consider how you can establish a more dynamic link between the control testing and your control environment.
- Do consider that not every control test will result in an upgrade/downgrade of the control environment rating, however the process for making that assessment should exist.



QUESTIONS