COMPLIANCE PRACTICE NOTE ONE
Assurance

GRC INSTITUTE
GOVERNANCE • RISK • COMPLIANCE

Preamble

GRC Institute Practice Notes provide advice to compliance practitioners on how to address Critical Success Factors stated in our Three Lines of Accountability paper. A copy of that paper can be found here. The Three Lines of Accountability is a business risk model which reinforces accountability at all levels of an organisation for governance, compliance and risk management.1

GRC Institute Practice Notes are written by members for members.

This Practice Note provides a recommended approach on how to design and deliver an assurance program.

Assurance – as defined in the GRC Institute Three Lines of Accountability model - refers to the overall controls monitoring, testing, review, and audit process across all three lines to provide evidence to the governing body and senior management on the effectiveness of compliance controls.

Guiding Principles

A successful assurance program includes the following elements:

- Purpose and clarity on what is being measured, assessed, and verified - and why
- Clearly defined programs in each line, especially lines one and two
- A framework that sets out each step in the assurance process
- Structured coordination and information sharing between all three lines
- Clearly drafted reports that engage and inform the reader

[1] The model was originally known as the 'Three Lines of Defence' and more recently, just 'The Three Lines.' The GRCI Institute renamed the model to reinforce the key element of ownership of all three lines to deliver an effective business risk model.

Approach

The assurance program provides empirical evidence on the extent to which the organisation can rely on the effectiveness of compliance controls and how it is really operating.

A successful assurance program will show the difference between documented compliance controls and what is being done in practice. Compliance controls can only support the business if they are well designed and properly executed. The assurance program will show if that is the case and provide a dynamic assessment of the compliance health of the business at a point in time.

It is recommended the framework for Three Lines of Accountability will include the following:

Define the assurance objectives and scope

Clearly state what you want to monitor, how it will be measured, the type of assessments that will be undertaken, how the outcomes are verifed and why the assurance program is necessary.

The 'why' is critical. Unless the business, senior executives and the board understand the purpose of the assurance program and why it is necessary to be in place, securing support to develop, expand or even continue the program will be difficult. A clear statement of the objectives of the assurance program will provide context to the reported results and any recommended remediation actions.

The challenge is selecting the most impactful controls within the compliance framework to test, monitor and measure. We suggest:

1. The first document to review is the compliance risk register. This register includes your obligations, regulatory requirements, controls put in place to address the risks, and an assessment of the residual risks as a result of implementing those controls. Consider the compliance risks with a high inherent risk, as control failures against these risks will potentially have the greatest impact on the business.

2. Consider controls that have a residual risk which is outside your stated risk appetite for inclusion in the assurance program.

3. Consider what information senior management and the board need to know about the effectiveness of the compliance program and the impact to the business. Where possible, engage with business leaders to help set the assurance objectives. Not only will this result in better engagement when presenting results, it can also help where adverse findings may require a request for additional compliance funding or resources.

Document the assurance structure across the lines

A successful assurance program is built on coordination and cooperation across all three lines. Line 1 (business) and Line 2 (Compliance, Legal and Risk functions) should discuss and agree on the structure of the assurance program, and how the two lines will assist in providing and analysing the data. While Line 3 (Internal Audit) operates independently based on an audit timetable, discussion between the three lines on the method and timing will assist when seeking co-operation and support from staff providing information for testing.

As stated at Table 1 of the GRCI Three Lines of Accountability paper (replicated as the attachment to this Practice Note), Line 1 should be structured to undertake management monitoring of routine issues that may cause loss, reputation damage, or a breach. This should be supported with resources in the business that will readily identify issues that may arise from time to time, which includes addressing any potential and/or non-systemic issues.

Line 2 assurance responsibilities are more extensive and designed to leverage and rely upon Line 1 data and results, not replicate them. As shown in the attachment, the structure of the Line 2 testing program should focus on effectiveness testing of controls and thematic reviews. Unlike ongoing monitoring, thematic reviews are generally triggered by an event – such as a response to new regulations, a breach, and changes in the organisation (usually people, process or product).

There is no 'one size that fits all 'when designing the assurance structure. It should consider the different types of assurance undertaken by each line and how they can be relied upon by the other lines.

Identify information sources

The assurance program should clearly identify the source of the data to be reviewed. Ideally, Line 1 data should be obtained from automated reports that provide information on the agreed compliance risks that are being monitored. These reports can be specifically designed for this purpose or obtained from existing reports that provide the information.

Line 2 data is often sourced from existing management reports or information supporting management certifications. Many companies require functional and business leaders to attest on a quarterly basis that key risks or controls have been reviewed and any issues reported. The working papers or reports supporting those certifications provide important source data that can be used individually or with other data points for analysis. Thematic reviews on specific risks or controls can also include onsite reviews and reports specifically prepared for detailed analysis.

When identifying your information sources, look to data that is built into the business objectives and productivity measures. This information is generally reliable (as it is used for performance metrics) and typically produced on a frequent basis – enabling trend analysis by examining data over time.

Determine how information will be collected

Protocols should be put in place as part of the assurance program on how the data will be collected and used. Report templates should be created to ensure consistency of collection and ease of analysis. Creating new templates for each review can result in significant rework and resistance by data owners in providing new or updated data requests.

Assurance frequency

All three lines should produce an annual assurance plan. Line 3 will typically issue an independent plan; Lines 1 and 2 can produce separate or a combined plan to show how the data will be used by both lines. Publication of the plan will reinforce to the business the purpose of the assurance program; how the work undertaken by each line supports each other and provides valuable insights for the business on the need for an assurance program across all three lines. The program is not one where one line is checking the work of another line. Each line is undertaking a different form of assurance that support and does not replicate work done in another line.

Analysis

This is the critical part of the assurance program. Once the data has been obtained it must be clearly analysed in order to develop a report outlining the results. The analysis should look for any red flags, potential systemic issues, and the need for further data to clarify any anomalies in the results. Given the nature of the data obtained, detailed analysis is generally undertaken by Lines 2 and 3 when producing their reports. Consultants or contractors may be used to assist small companies or larger projects.

Documenting results

Think carefully how the results are presented. A successful report quickly provides the key points to the reader. A recommended report structure would include an executive summary, commentary on the findings supported by graphs and tables which clearly illustrate any trends or key points and recommended next steps. Avoid presenting raw data or complicated charts.

Communication and engagement

Don't waste your effort by failing to engage others with the result! Your assurance compliance report should first be shared with the business to discuss any findings that could cause concern and may require more detailed discussions. The final report should also form part of a regular reporting program, such as compliance or risk committee meetings or other management meetings.

Reporting and presentation to management/board

Use the compliance assurance report to showcase to management/board how the compliance program is working and areas that require attention. While the report should be clearly written so that it can effectively speak for itself, come prepared to the meeting to highlight the key points and draw attention to the specific data points or graphs that require more attention. Think about the questions that management/board are most likely to ask and be prepared to answer as best as possible with the available data.

Outcomes

- Insights into the effectiveness of the compliance program
- Empirical evidence on controls that require remediation
- Meaningful data and reports to use in discussions with the business on how to reduce compliance risks
- Indicators of behaviours or structures that warrant further investigation
- Structured engagement and reporting to senior management/board on critical issues

Tips

Only measure what is important, not the most easily measurable

Go back to the objectives of the assurance program. Is the data actually providing the information you need to understand the risks in your compliance controls and programs – or are you merely using data that is easy to collect? For example, many companies monitor the number of people who complete their compliance training. But what does that actually measure and why is it important to the organisation? Quantitative assessments, such as training results, are only meaningful when linked back to behavioural outcomes reflected in complaints, regulatory enquiries or other reputation risk factors that are important to the entity.

Measure outcomes not inputs

The assurance program should not focus on how many people or how much money was spent on achieving an outcome but obtaining evidence that the results were achieved.

Avoid the Cobra Effect

The Cobra Effect[2] refers to developing a solution to a problem which actually makes the issue worse. This effect can also occur when assurance programs do not continually evolve to keep pace with the actual or potential risks.

[2] During the colonial occupation of India, the British offered a reward for dead cobras to stop an infestation in Delhi. This resulted in people creating cobra farms in order to claim the reward. Once the reward ceased the cobras were released, creating a worse problem than the original situation.

Assurance programs that continue to measure the same risks can result in bad actors looking to take advantage of other control weakness, knowing they are not being assessed or reviewed. So continually measuring one potential risk weakness can result in another being created.

Challenges

Poor data quality or analysis

Your results are only as credible as the data that is being relied upon. Schedule frequent reviews with the data owner to ensure that the data is reliable and accurate. Also work with the person undertaking the analysis to ensure that the results are consistent, free from confirmation bias or lowering of standards (see below).

Confirmation bias

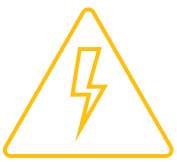
Focus on what all the information tells you, not just on the facts that support your assumptions. Omission or distortion of data may result in poor decision making, due to the fact that incorrect conclusions of compliance risks were made.

Maintaining standards

Resist any attempt to manipulate results through lowering standards to give the appearance that controls are effective. Examples include lowering pass marks on compliance testing, number of complaints that would generate an adverse finding or CPD hours.

Management denial

When presenting your findings to management or the board, there may be pushback or challenges, especially if the results indicate additional resources or changes are required. Prepare for these questions by asking them yourself. How confident are you of the quality of your data? Are there any potential weaknesses in the analysis? Also look to external data to benchmark your results in the context of your industry.



Disclaimer

Contact us

Naomi Burley, CEO
naomi.burley@thegrcinstitute.org

Find us on LinkedIn: GRC Institute or go to our website
http://www.thegrcinstitute.org

Attachment

Assurance Definitions across the three lines

Term	Definition	Potential Frequency[3]	Line Owner
Non independent Management Monitoring	• Repeatable checking by the business of routine issues that may cause loss, reputational damage or a breach. • Often automated e.g. monitoring of training completion by management or monitoring trends as part of a dashboard review.	High (daily, weekly, monthly)	Line One
Independent Compliance Testing, Review and Monitoring	• **Testing:** The testing of compliance controls in accordance with a defined sample methodology. The specific controls in scope are documented and operationalized by Line 1. The testing includes design effectiveness testing and operational effectiveness testing. • **Review:** Structured or thematic reviews at a specific point in time of a Compliance process risk or control by Compliance based on risk assessment. This method provides a better understanding of how well the controls are designed to mitigate the compliance risk based on the annual plan. • **Monitoring:** Consistent with the monitoring definition at Line One but is conducted independently from the business. This form of assurance does not focus on assessing design or operating effectiveness and therefore is not considered either a review or testing.	• High • Medium (Quarterly, Bi-annually or annually)	Line Two
Audit	Performs auditing process in accordance with an annual plan and provides an independent assessment of the risk management and internal control systems.	Low: contingent on risk assessment. Range from 1-3 years.	Line Three

[3] 'Potential frequency' stated in this table is a guide only and should be adjusted to suit the type and size of the business.