The governance world is increasingly focusing on the relationship between organisational culture and risk. It’s also focusing on approaches to gaining deeper insight into the alignment between the culture throughout the organisation and the one described in the boardroom. There is little doubt that an organisation’s culture can either overwhelm, or reinforce, the carefully placed operational controls that company leaders rely on to manage and monitor their organisations. So it makes sense that a considerable amount of effort will be expended to establish, nurture and monitor culture. The question becomes, who should expend this effort and what specifically should they focus on?

While internal audit has long incorporated the impact of culture into its risk assessment and audit-scoping activities, the profession took a significant step forward into the culture discussion with the Institute of Internal Auditors (IIA) February 2016 release of its global thought leadership piece ‘Auditing Culture – A Hard Look at the Soft Stuff’. Within this piece, the IIA strongly encourages internal auditors to include the auditing of culture as a core component of their audit approach. Internal auditors have an important role to play in providing...
an organisation’s governing body and senior management with independent assurance in the area of corporate culture. However, organisations should proceed with caution and avoid inappropriately placing too much responsibility on the internal audit function for obtaining insight into the state of their culture.

To best answer the question of what role varying parties should play in establishing, monitoring and validating organisational culture, it’s appropriate to revisit the three lines-of-defence model, designed to add efficiency and accountability in matters of organisational governance. As the IIA described in its January 2013 position paper, ‘The Three Lines of Defence in Effective Risk Management and Control’, the responsibility can be broken down accordingly: the first line of defence are management controls, the second line of defence are risk and compliance oversight functions established by management and the third line is independent assurance (typically fulfilled by internal audit).

Senior management and a company’s governing body, while not formally considered one of the ‘three lines of defence’, are described by the IIA as having “responsibility and accountability for setting the organization’s objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to best manage the risks in accomplishing those objectives”. By anchoring ourselves in this framework, we can see that the internal audit has an important role to play in addressing organisational culture, as it does with any risk facing an organisation. However, internal audit is just one piece of a broader governance puzzle.

To define the appropriate role of internal audit in auditing culture, let’s first reflect upon its role as part of the third line of defence, which is designed to provide independent assurance. The Merriam-Webster dictionary defines assurance as “the state of being sure or certain about something”. This quality of certainty is why internal auditors seek objective facts when conducting their audits, and compare their test results to documented standards, frameworks, policies and regulations. It’s difficult to provide stakeholders of internal audit assurance when no basis of comparison exists. At that point, internal audit might be sharing valuable opinions, but little in the way of certainty. So, for internal audit to effectively fulfil its role relative to auditing an organisation’s culture, senior management and the governing body need to clearly define, in concrete terms, their desired culture (i.e., what does ‘good’ culture look like?). Then, implementing processes and controls to align behaviours with the desired culture will enable companies to meet their first line of defence requirement.

Organisations also need to establish oversight and monitoring activities to provide senior management and the governing body with a basis from which to develop an opinion as to the health of the organisational culture (aligned with however senior management and the governing body have defined a ‘good’ culture), thus meeting their second line of defence obligations.

Internal audit cannot, and should not, be relied upon as the primary source of insight or control regarding an organisation’s culture. For internal audit to effectively fulfil its role of supporting senior management and the governing body’s ability to monitor and assess organisational culture, each of the other pieces of the governance puzzle needs to have fulfilled their roles as well. If stakeholders are looking to internal audit to provide them with their original understanding as to whether the organisational culture is ‘good’ rather than validating their established opinion on the matter, then internal audit has been placed in
a perilous situation. At that point, the organisation has already demonstrated a failure to dedicate sufficient effort and resources to one of the areas that stands to have the largest impact on their organisation’s future success.

When dealing with a topic as important, and judgmental, as culture, there simply are no short cuts. The challenge with assessing organisational culture is that it tends to play in the ‘grey area’ of governance. Organisational culture helps shape how people behave and the decisions they make within the parameters set by existing policies, processes and controls. If someone operates in violation of a documented policy, law, regulation or organisation procedure – it’s fairly easy to determine non-compliance and to conclude that such failures are inconsistent with an organisation’s desired culture.

However, assessing the health of a culture is much more difficult when demonstrated behaviours can vary significantly between two environments, yet both fall within the parameters of documented requirements. What one organisation views as a desirable cultural characteristic, another might define as unacceptable. That can also be said within the same organisation. For example, a manufacturer might desire a very conservative, risk averse culture within its engineering department, but look for aggressive behaviours within its sales and marketing teams. Assessing culture isn’t as easy as simply identifying your organisation as ‘conservative’ or ‘aggressive’ (acknowledging that neither of those characteristics is inherently wrong, or even the desired nomenclature), because the desire and definition might vary between internal environments. For internal audit to provide observations of value to its stakeholders, those responsible for setting the culture of an organisation must first define expectations across each part of the business, as well as the observable behaviours that illustrate consistency with, or variance from, that expectation. If cultural expectations aren’t developed, clearly communicated and further reinforced by controls and processes throughout the organisation, the organisation effectively defers to internal audit the responsibility to define cultural expectations and the factors used to determine how alignment is sufficiently demonstrated. In other words, internal audit will have been pulled from the third line of defence and spread across all three lines of defence – not an effective or efficient approach for an area as judgmental and politically charged as organisational culture.

Internal audit is one important piece of an extremely critical governance puzzle. Once the other pieces of the puzzle have been put in place relative to an organisation’s culture, there is tremendous value to be had from internal audit providing an independent assessment of the mechanisms that senior management and governing bodies are using to monitor and assess the organisation’s cultural health. Every organisation, and its key stakeholders, will significantly benefit from the adoption of a consistent and comprehensive approach, including the appropriate use of internal audit, to managing the risks associated with organisational culture.