Risk culture

The role of internal audit

2015 is the year of culture within financial services. Regulators globally have highlighted that culture has accelerated up their agenda as part of addressing what they perceive to be major conduct and control failures that could have a systemic impact if not addressed properly.

Definitions abound as to what culture means. Put simply, firms see it as "the way we do things around here" – that is, the embedded norms and patterns of behavior.

It is clearly heavily influenced by the firm's overall organizational culture and each employee's own ethical values. Regulators have been relatively expansive in how they talk about culture, but their core focus is on those behaviors or behavioral mechanisms that influence the firm's risk profile – what some call risk culture. (See “EY's risk culture model” on page 4.)

Supervisors globally have started to embed culture into their supervisory approach. Some, like those in Australia and the Netherlands, have explicitly evaluated risk culture as a discrete topic for discussion. In other countries, such as the UK and the US, it is being layered into ongoing supervisory dialogue around risk governance.

In essence, regulators are trying to get answers to three questions:

1. Does the firm have a strong risk and control culture?
2. Can it evidence that its actual risk and control culture aligns with the desired culture?
3. What steps are being taken to address areas where actual culture does not align with desired culture?

Risk Governance 2020

EY believes financial services firms face a sea change in how they approach risk governance.

Risk culture is one component of this overall effort.

The transformation required will take a comprehensive, multi-year effort to substantively complete. To remain at the forefront of today's market, firms should adopt an integrated approach that capitalizes on the value gained from upgrading risk governance: placing an equal focus on financial and nonfinancial risks in the short and long term, embedding evolving regulatory and supervisory expectations, and delivering tangible results in a cost-effective manner. We call it Risk Governance 2020: a shift from satisfactory to effective and sustainable.
Supervisors will assume every firm will say it has a good culture. However, evidencing it is another thing, as is detailing plans to resolve areas in need of improvement – and everyone has them.

Internal audit has a central role to play in addressing culture. It routinely experiences behavioral and cultural issues in its ongoing audit work, such as management’s responsiveness or its proactive focus on controls, but traditionally it has not explicitly evaluated or commented on them. This is beginning to change. New approaches are being implemented to allow internal audit to influence culture and help engender a strong risk and control environment. These changes also help enable internal audit to constructively engage regulators on cultural issues.

Differing approaches

To determine the best way to address risk culture, firms operating in the UK and increasingly elsewhere are looking at the issue from the perspective of internal audit. Guidance issued by the UK Chartered Institute of Internal Auditors in 2013 on the performance of internal audit in financial services included a recommendation that internal audit evaluate and report on risk culture.1 2015 is the first year this requirement applies. The pressure for change is increasing beyond the UK: because so many large foreign firms operate in the country, changes are quickly being exported.

Industry practice is still emerging. Some firms have chosen to wait. Others have limited their input to managers’ attitudes about controls in firmwide annual performance reviews of senior and middle management. Others have added a question or two on behaviors to audit questionnaires.

Where firms’ internal audit teams have adopted approaches to systemically evaluate behavioral and cultural factors, they have chosen one of two approaches:

- **Management controls assessment (MCA):** Over and above the control environment rating, some firms have developed a distinct perspective on management’s overall control awareness, with varying levels of formality.

- **Embedded in the audit approach:** Some firms – for example, in the UK and some in other markets – have fully embedded culture into the overall audit approach (spanning risk assessments, audit planning and the audit program) to be an integral part of every audit.

Each approach takes a narrower definition of behavior than an overall firmwide risk culture framework would, as it zeroes in on behaviors that are clearly linked to the quality of, and importance placed upon, the internal control environment, such as control awareness and understanding. Yet attitudes and behaviors related to internal controls are central to questions of how culture can affect risk and are, of course, at the core of internal audit’s mandate and expertise. A well-implemented approach along any of the types described below can materially contribute to a stronger control culture and provide evidence to supervisors that internal audit is taking culture seriously.

---

Building a robust management controls assessment (MCA) is challenging

A stand-alone commentary or rating of management's focus and support for controls is increasingly a common starting point.

By calling out internal audit's view of the extent to which management embraces the control environment, MCAs can incentivize management to be more aware of key risks and how well existing controls address those risks. This is even more important in the context of regulatory and supervisory pressure for stronger frontline accountability for risk. An MCA can recognize a proactive management approach in identifying and rectifying control weaknesses, and it can help promote an open transparent approach.

A selection of objective and subjective factors can be used to make the assessment more robust, defensible and evenly applied. Factors often focus on risk identification, risk remediation, and governance and attitude.

While objective data should form the foundation (e.g., percentage of responses to audit issues overdue by 90 days or longer), somewhat subjective factors may also be necessary (e.g., evaluating the difference between constructive engagement on the facts contained in draft internal reports to confirm accuracy versus adversarial and objectionist behavior). The factors may have to be weighted to focus appropriate attention on each one, and their weightings may change between audits.

Beyond the selection of criteria, major methodological decisions have to be made related to the output. Should it simply be commentary in the overall audit report or a stand-alone report or section? Should management awareness have its own rating or be factored into the overall audit rating? Should control awareness be covered in every report or aggregated over time and reported periodically (e.g., quarterly by line of business)? How detailed should the written guidance be for auditors? How should the results be communicated and to whom? What action should be required to address less-than-satisfactory ratings?

Making the right decisions on the factors and design will greatly influence the way the organization accepts MCA, as will strong communication and senior management support.

Figure 1: Illustrative MCA factors

<table>
<thead>
<tr>
<th>Risk identification</th>
<th>Risk remediation</th>
<th>Governance and attitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Ongoing management testing, monitoring and oversight processes validate that controls are appropriate and effective.</td>
<td>▶ There is a low percentage of past-due audit findings or repeat or reopened audit issues.</td>
<td>▶ Engagement of internal audit is constructive.</td>
</tr>
<tr>
<td>▶ There is proactive self-reporting.</td>
<td>▶ Well-documented, quality action plans tackle the root cause as well as the issue.</td>
<td>▶ Management challenges and oversees remediation plans.</td>
</tr>
<tr>
<td>▶ Comprehensive risk assessments incorporate internal audit's control environment assessment.</td>
<td>▶ Enhancements implemented in response to audit findings are sustained over time.</td>
<td>▶ Control and remediation budgets are appropriate, and front and second lines are well-resourced.</td>
</tr>
<tr>
<td>▶ All risks in the business or function are covered, including conduct and other nonfinancial risks.</td>
<td></td>
<td>▶ There is a positive response to internal audit.</td>
</tr>
</tbody>
</table>
EY’s risk culture model

EY has developed its own view on what constitutes a holistic approach to risk culture. It comprises two core and complementary elements:

- The behaviors that drive risks, such as being responsible and accountable for one’s own actions, as well as being collaborative, ethical and compliant
- The mechanisms that influence behavior

See Risk Culture: much ado about something, EY, June 2015.
Embedded in audit approach

Those firms that have gone the furthest have embedded behavioral or cultural factors explicitly into their audit methodology, both in how audits are planned and performed. Few firms have gone this far, but others may follow as the profession's approach to culture develops.

Such a change has to be implemented over time. Firms have to determine what their focus will be. For instance, what behaviors and culture mechanisms will be part of the audit methodology? What specific factors will be assessed comprehensively and consistently? The proposed approach needs to be well-documented, because precise words matter with such subjective issues as culture – firms learn that risk culture manuals have to be created and audit methodologies redrafted. In doing so, existing corporate documents, including codes of conduct, value statements and performance assessments, also need to be evaluated to validate that the proposed approach to audit culture and behaviors is congruent with the firm's existing overall organizational culture, style and processes. The proposed revised audit approach should be syndicated beyond audit to make the new audit methodology stronger and to get the necessary buy-in.

Before undertaking a major overhaul, sometimes internal audit conducts one-off thematic audits, such as risk reporting or deep-dive audits, on areas that audit perceives to be high risk culturally.

Any proposed revisions to the audit approach need piloting so that it is fully vetted and tested. They could include some of the following:

1. A “horizontal” audit to test the methodology translates across business functions
2. A “customer-facing” audit to test the methodology with the first line of defense
3. A “support function” audit so that the methodology effectively tests back-office operations
4. A second-line-of-defense unit
5. An audit that requires interaction with executive management
6. Where relevant, an “international” audit so that the methodology works across different local subcultures

Only after these pilots are completed will gaps and flaws in the approach emerge; refinements based on actual experience are inevitable. Several iterative pilots may be needed. Once the pilots are complete, the approach can be expanded to include additional business units and processes; over time, the approach can be applied to the whole audit universe.

Later, as the planning process comes around, findings from the completed audits can be woven into the audit planning process so that risk culture influences audit plans as much as individual audits.

Challenges

There is no silver bullet. Firms will decide on their chosen approaches depending on their current situations and histories. Some will opt to rely solely on an MCA, at least for now. Others will determine that, if done with care, they can move straight to embedding culture into their audit methodology. What’s important is that firms understand the challenges of each approach as they determine how they will proceed.
### Figure 2: Challenges and critical success factors

<table>
<thead>
<tr>
<th>Factor</th>
<th>Management controls assessment (MCA)</th>
<th>Embedded into audit process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prevalence</strong></td>
<td>➢ Being used by some Australian banks and most large UK banks&lt;br&gt; ➢ Being used by some US banks, while others are considering them</td>
<td>➢ Performing audits of firmwide or business-unit-wide culture programs&lt;br&gt; ➢ Embedding culture into audit (particularly UK banks or global banks with UK operations)</td>
</tr>
<tr>
<td><strong>Challenges</strong></td>
<td>➢ Selecting and consistently applying factors&lt;br&gt; ➢ Determining how to document and communicate findings&lt;br&gt; ➢ Developing an appropriate rating scale and manner in which the MCA rating affects overall audit rating&lt;br&gt; ➢ Determining how to use MCA ratings in periodic geographic or line-of-business-level reports&lt;br&gt; ➢ Factoring MCA ratings into audit planning process</td>
<td>➢ Building a methodology and tools that are as robust as other internal audit approaches&lt;br&gt; ➢ Training internal audit teams on how to apply methodology&lt;br&gt; ➢ Managing relationships with senior management at audited entities given explicit focus on culture findings</td>
</tr>
<tr>
<td><strong>Critical success factors</strong></td>
<td>➢ Using clearly articulated and well-understood factors&lt;br&gt; ➢ Deploying a systematic rating methodology</td>
<td>➢ Piloting and iterating new approaches&lt;br&gt; ➢ Getting senior internal audit executives strongly involved&lt;br&gt; ➢ Communicating clearly and continually&lt;br&gt; ➢ Having patience</td>
</tr>
</tbody>
</table>
Successfully building culture into the internal audit approach

To the extent the firm is developing an enterprise-wide risk culture framework, internal audit can contribute. However, internal audit must do so in a way that maintains its independence and objectivity given that, in some jurisdictions, it has to evaluate the firm’s risk culture and risk governance frameworks (e.g., in the UK and US, respectively).

Regardless of the firm’s overall approach to culture, internal audit can build culture into the audit process, thereby playing a role in influencing necessary cultural change and expanding the view of risks and controls at the audit committee and firmwide.

There are some common key success factors:

- **Internal audit senior leadership has to play a key role** in championing the approach, in guiding the conclusions and in engaging management in findings on audited entities.

- **Stakeholder support is required.** Audit committee support, from the onset and ongoing, is important, as is support from senior management and the key functions, notably risk, compliance and human resources.

- **Ongoing, clear communications are critical**, as is training. This means communications within internal audit and across the company.

- It’s important to be **transparent on the intent**, approach and usage to garner and maintain support. What is internal audit trying to achieve, and how does the proposed approach meet that goal fairly and professionally?

- **Consistency is paramount.** Internal audit already routinely gets questions from audited entities about whether they are being treated the same as other parts of the firm, especially (and perhaps only) in critical audit reports. This tendency will be exacerbated in the context of evaluating behaviors.

To the extent a broader firmwide effort on culture has distilled and agreed-upon desired risk behaviors for all employees, it is important that internal audit’s chosen approach reinforces those behaviors.

---

**EY’s Risk Governance 2020:**
a shift from satisfactory to effective and sustainable

www.ey.com/rg2020
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Ernst & Young LLP refers to the individual client-serving member firms of Ernst & Young Global Limited operating in the UK, US. Ernst & Young refers to the client-serving member firm of Ernst & Young Global Limited operating in Hong Kong. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace

Nearly 43,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. EY professionals in our financial services practices worldwide align with key global industry groups, including EY’s Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients. With a global presence and industry-focused advice, EY’s financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2015 EYGM Limited.
All Rights Reserved.

CK0979
1504-1441892
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.