According to a 2013 survey called “Exploring Strategic Risk,” conducted jointly by Deloitte and Forbes Insights, reputation risk is now rated as the highest impact risk area. This is from a survey of 300 executives equally split among the Americas, Europe/Middle East/Africa, and Asia/Pacific.

Similarly, the fourth annual directors’ survey (2013) from Eisner Amper also identifies reputation risk as the number one risk (aside from financial risk). This risk was named by a high percentage of directors, ranging from 65 percent (private equity owned) to 77 percent (not-for-profit). Privately held and publicly held entities fell in between these numbers.

In this Eisner Amper report — called “Concerns About Risks Confronting Boards” — they state:

“Our data shows that the most significant concern for boards today is the issue over which they have increasingly less control: public perception or, as it’s become known, reputational risk.”

Now couple this concern with another common theme from directors: their desire to have internal audit focus on strategic issues that are important to the organization overall. When internal audit is willing to take up the challenge and focus on these key strategic risks, this helps not only the board but also the perception of internal audit within the organization. In 2011, Crowe Horwath published a white paper entitled “Taking Internal Audit to a Strategic Level.” In it, they said:

Internal audit can play an essential role in the shift to a proactive risk management model by integrating the identification and assessment of enterprise-wide risk into the audit plan. The insight internal audit gains from these activities and communicates to senior management and the board of directors can make risk management efforts more relevant, reliable, and resilient. It can also move internal audit into a strategic advisory role through dialogue that helps management better understand risk in relation to the vision and objectives of the organization.

What is reputation risk?

There are quite a few definitions, but they are generally comparable. Businessdictionary.com defines it as “the risk that a company will lose potential business because its character or quality has been called into question.” Similarly, thelawdictionary.org defines it as “the risk that a company may lose business when its character or quality of products is questioned.”

Investopedia.com has a longer description:

“An threat or danger to the good name or standing of a business or entity. Reputational risk can occur through a number of ways: directly as the result of the actions of the company itself; indirectly due to the actions of an

CHARLES D. SCHROCK, CPA, CIA, CRMA, is a senior vice president at Inland Bank and Trust in Oak Brook, IL, where he is both the senior risk officer and the chief audit executive.
employee or employees; or tangentially through other peripheral parties, such as joint venture partners or suppliers. In addition to having good governance practices and transparency, companies also need to be socially responsible and environmentally conscious to avoid reputational risk.6

Not all aspects are consistent in these definitions and descriptions, but a few themes are repeated. First, there is often a reference to “loss of business” but that isn’t necessarily a defining factor. As shown in the Eisner Amper survey, not-for-profit (NFP) board members are the most concerned about reputation risk. For NFPs, reputation risk is critical because a damaged reputation can dry up funding sources in a heartbeat.

Another common theme in these definitions and descriptions is the organization’s character or quality being called into question. However, reputation risk is a very broad concept. Character and quality are undoubtedly related to reputation, but these are not the only related concepts that drive reputation risk. Six general concepts often emerge when discussing reputation risk.

1. Social media and speed of communication: Many executives link the speed at which bad news can travel to being a prime factor in their concerns about organizational reputation.

2. Maintaining a public image: When an organization attempts to cultivate a particular public image (e.g., “safe for children,” “lowest price,” or anything else), its actions need to be consistent with this desirable image. Reputational damage can arise when actual organizational strategies fail to align with this stated public persona.

3. Social responsibility: This could include something as simple as a general public perception of what it means to be responsible. Alternatively, it might be impacted by specific technical assessments from third-party groups relative to environmental impact and sustainability. It is a special case of “maintaining a public image” described previously.

4. Ethical behavior: Even starting in small ways, an organization’s image of fair and equitable dealing (or lack of it) can grow quickly and become very persuasive. Public perception of fair dealing can impact a business strategy. Some internet retailers have chosen a strategy of allowing returns with no questions asked. Some even provide free shipping for returned merchandise as a way of building a broad perception of fairness and high ethics.

5. Disaster recovery and business continuity: Public perception can result from an organization’s ability to respond effectively to big (and often very public) problems. While bad responses to such problems can be extremely damaging, good responses can sometimes enhance an organization’s image far beyond the damage from the problem itself.

6. General organizational competence: If the organization is seen publicly as being inept or bumbling in one area, this may quickly evolve into a broader perception of incompetence. An example of this might be a retailer that, for a two-week period during which it was changing its ERP system, was consistently shipping the wrong products. While (from the company’s point of view) the specific problem may have been short-lived and contained within a very small activity, the very public knowledge of this shortcoming may result in significant reputational damage.

When contemplating an audit of reputation risk, it is important to at least consider all of these potential issues when establishing the scope for the review. However, before finalizing any audit scope, it is best to discuss these concepts with executive leadership and audit committee members in order to determine which of these (or potentially others that had not yet been considered) should be the focus.

Getting management on board
The more a person looks at this topic, the more it becomes apparent that reputation risk is not a simple risk to be analyzed and mitigated. Reputation risk is a complex and layered risk environment.
Unlike other more common risks, reputation risk is often not an “event” to be avoided. Instead, reputation is commonly damaged by an aggregation of other risks, sometimes over the long term. These other risks that lead to reputation damage can, perhaps, be avoided or mitigated with an appropriate internal control environment.

Before beginning an actual audit of reputation risk, the most beneficial activity may be simply facilitating a discussion. As indicated in the surveys mentioned earlier in this article, reputation risk is near the forefront of many executives’ minds. The auditor might wish to tap into this concern to create a reasonable and rational dialogue.

Facilitating communication may not be considered a primary role of internal audit. It is, however, an important skill for every member of the senior leadership team — including senior internal audit leaders. It is especially important here because the basic concept of reputation risk may not be consistent across the organization. Some executives may equate reputation risk with viral comments on social media. Others may think more along the lines of responses to faulty products. Management cannot reasonably address reputation risk until there is agreement on what it uniquely means within the organization.

Often, an internal auditor can help the organization develop its view of reputation risk through internal audit’s broad view of processes and risks. This is best done by engaging the senior leadership team in a general discussion. During such a discussion, certain questions might be useful, including:

1. What components of our public image are most important? How could inappropriate strategies or poor management decisions spoil that image?
2. How do we use social media? Do we encourage its use? Do we monitor those sites where our customers or other stakeholders might aggregate? Is someone specifically responsible for seeking out and responding to unfavorable social media comments? Do we prefer to aggressively contra-
dict unfavorable comments or do we want to embrace them as part of a mutual learning environment?
3. Do we have a code of conduct supported by a functioning whistle-blower process? Do we set the appropriate expectations about how the organization will ethically conduct its operations? How will we respond if there are allegations that a segment of the organization is straying from our ethical guidelines?
4. Do we maintain an overall performance management environment where we track key performance indicators? Would we know if certain basic business activities stray significantly from desired levels? How would such variances from desired activity get elevated and addressed?
5. Does our industry (or our organization specifically) have certain “extinction” scenarios that may be beyond our control? These are events that are so insidious that they could mean a quick end of the organization. What are these scenarios? What plans do we have to specifically address these scenarios? This is often far more complex than simple disaster recovery or business continuity.
6. Are we entrusted with highly valuable, dangerous, or classified materials? If we failed to adequately safeguard these materials, would this create a public outcry?
7. Do we maintain sensitive, confidential customer or industry data? Would the inadvertent release of this information destroy a public expectation of confidentiality?
8. Do we have effective disaster recovery and business continuity? Have we considered all reasonable events and scenarios?

As part of these discussions, the auditor can record where controls are presumed to exist in order to help prevent or mitigate these risks. Even where controls are lacking, management may presume to have other mitigation — such as a general understanding of the organization’s ethical standards. Document all
of these mitigation and control activities, as they will serve as the basis for an audit review.

It is useful to project an auditor’s healthy skepticism during these discussions. When management says “that scenario could never happen,” it can be very beneficial to offer a gentle push-back of “that doesn’t seem so impossible to me.” The idea, of course, is to avoid people clinging to what’s likely to happen and focus more on what could reasonably happen. Also, it can be helpful to keep the management team focused less on its view of the risk scenario and more focused on the public’s perception of that scenario.

How can internal audit help address reputation risk?
Once the auditor has a reasonable understanding of what reputation risk means to the organization, it is time to determine how internal audit might help.

First, an auditor needs to gain commitment and support from senior management and the audit committee. From the prior discussion, management may
recognize the existence and importance of reputation risk. However, that recognition may not equate to support for an audit of those risk elements. One way that an auditor might gain this support is by recapping a few points:

1. Internal audit delivers the greatest benefit when it is providing independent assurance relative to the organization’s most significant risks.

2. Reputation risk arises quickly and unannounced. If the process for addressing reputation risk is not functioning as intended, there may be no opportunity to fix it. It may be too late.

3. Unproven assumptions can be disastrous. Executive leadership may wrongly assume that others in the organization are either performing certain activities or will react properly in the event of a significant reputation risk scenario. These assumptions need to be explicitly validated.

4. There are often specific control processes that are expected to address lesser risks before they become so pervasive that they might damage overall reputation. These controls and reporting processes should be evaluated for effectiveness.

   The important point is that reputation risk can be prevented (or, at least, mitigated) when appropriate processes are in place. Internal audit is the right organizational unit to evaluate these processes — and provide independent assurance that such processes are efficient and effective.

   Conducting a review of this nature may present challenges to the internal audit organization. An audit review of reputation risk may force internal auditors outside of their comfort zones. This will entail far more than common audit activities such as reviewing documents for proper approvals. For this review, the auditor may prefer to imagine that he or she shares the CEO’s view of a holistic organization and the need for a functioning, coordinated process.

   If the auditor were able to facilitate the management discussion that was described earlier in this article, certain processes and controls might have emerged. If such a discussion was not possible (or did not include all of the right people), then the auditor might need to make assumptions about how the mitigation processes should work.

   In any case, there are objectives that the audit should generally include. This list of potential audit objectives may need to be modified for each situation.

   To meet certain audit objectives, it may be appropriate for the auditor to engage subject matter experts. For example, to be able to validate the effectiveness of social media monitoring, it may be appropriate for the auditor to engage an organization that specializes in managing social media risk. Where IT-related issues are involved, it also may be appropriate to engage qualified IT audit specialists.

**Summary**

Reputation risk is a complex and layered risk environment. It is very much on the minds of executives and governing boards. In light of this (and its extraordinary potential impact to an organization), internal audit should include reputation risk within its audit plan.

Reputation risk presents certain challenges to the audit team. First, executive leadership may not be willing to invest time and energy (including internal audit time and energy) on a risk environment that they don’t fully understand. Second, its complexity may require more discussion (and less “testing”) than in a more typical audit. Third, it cuts across the organization and may be less contained within a particular area of responsibility. Audit recommendations may require cooperation and agreement from a number of people.

These challenges, however, are manageable. If approached properly, executive leadership will recognize the importance of reputation risk and express a desire to have some assurance about its potential impact.

Beyond the challenges, there are significant benefits. Perhaps more so than with any other audit review, it will be critical for the chief audit executive to maintain regular communication with
the executive leadership team as this review unfolds. Adding a reputation risk audit to the audit plan not only helps the organization prepare for a significant potential risk scenario, it also helps elevate internal audit as part of the senior leadership team.

NOTES