Internal Auditor Risk Watch Column, April 2009 Issue
The Matrix Revisited

By Larry Hubbard

A risk matrix is a commonly-used tool for documenting the analysis of objectives, risks, and responses. Typically a risk matrix focuses first on the inherent risks related to an objective — that is, all the risk events that could have an impact on achieving the objective, without regard to management's responses. The typical inherent risk matrix lists these risk events, along with a risk rating (e.g., high, medium, or low) of their potential impact and likelihood. Next, the matrix identifies management's response (i.e., controls) to each event and determines the overall adequacy of the design of controls. The central question of this assessment is, considering the risks identified and the responses management has in place to mitigate, or control, the risk events, is there a reasonable likelihood that the objectives will be achieved? Based on this assessment, auditors prepare an audit program to test the operational effectiveness of controls.

However, using a residual risk analysis approach that starts by identifying controls can make the risk matrix process more effective and efficient. In most processes and activities, identifying what already exists first is a more direct method. Plus, it is a more positive experience for auditors and managers, because the approach looks for good things first (controls) rather than bad things (risks).

Inherent Risk Matrix Shortcomings

Many auditors have used inherent risk matrices along with The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Internal Control–Integrated Framework* to evaluate the effectiveness of internal control over financial reporting as part of compliance with Section 404 of the U.S. Sarbanes-Oxley Act of 2002. For some, these matrices identify several shortcomings in the inherent risk format. For instance, it is easy to:

- Confuse risk with the absence or ineffectiveness of controls.
- Confuse impacts — the result of not achieving an objective — with risks that prevent achieving the objective.
- Go in a circle by identifying risks that are simply stated as the opposite of the objective.

Conversely, it is difficult and time-consuming to identify what could go wrong if there were no controls (inherent risk) because this is a theoretical question. In reality, there almost always are some controls in existence.

The result of these shortcomings is that people may identify areas in their inherent risk analysis that aren't truly risks that need to be dealt with. For example, in considering the business objective *safeguarding assets*, auditors may incorrectly identify the following as risks

- Not safeguarding assets (the opposite of the objective).
- Loss of assets (a result of not achieving the objective).
- Assets may not be available for use (an impact).
- The guard may not be awake (an ineffective control).
- There is no guard on duty or gates are not locked (missing controls).

After identifying these, auditors using this approach may overlook real risk events. In fact, in a business situation, determining real risks is difficult because there are already so many controls in place. Although the shortcomings of the traditional approach may not prevent auditors from developing an effective risk matrix, the process can take much longer and require several iterations. Moreover, the use of words such as *not*, *no*, and *lack of* can make this method appear to be a negative way to identify controls, thus potentially complicating the auditors' relationship with their clients.

Another shortcoming is confusion over the term *risk*. Although The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards*) measures risk in terms of its impact and likelihood, in practice the term may be used in many ways, such as:

- When some managers ask, "What's the risk to the organization?", the term *risk* really means "potential impact."
- Some audit departments use the word *risk* when communicating audit findings, as a measure of the importance of the finding.
- Some organizations define risk management as a function performed by managers to identify and address important events that impact achieving objectives.
- In some organizations, risk assessment is either a component of internal control or enterprise risk management — per COSO's definitions — or a method audit departments use to develop an annual audit plan.

As challenging as these issues are, management's perception of the inherent risk matrix is the biggest shortcoming of this approach. Managers may think that identifying risks, without considering the controls already in place, is a purely intellectual act, akin to reinventing the wheel. They may not react well to participating in a risk assessment process that ignores what they already have in place to achieve objectives. And they may not see any benefits from re-thinking controls from that inherent risk base. These managers have a good point: Existing systems, procedures, and policies are not going away, even if the auditors want to imagine a world without them.

In today's businesses, most processes and activities are well-controlled. Sure, there are control gaps, but policies and procedures, training, good hiring practices, clear roles and responsibilities, monitoring, and information systems are commonplace in business. If those controls are not present, or if an organization does not have good managers, then risks are always going to be

unacceptably high. In practice, the biggest risk for most organizations is existing controls not being executed.

The Residual Risk Format

With so many shortcomings, it is no wonder that most managers and workers, when asked to participate in a workshop to discuss inherent risks, regardless of the controls already in place, will find something else to do. However, many audit departments are finding that a simple shift in thinking, with a corresponding change in the risk matrix's format, can be much more successful. The residual risk approach begins by first identifying the controls already in place to achieve a business objective. Once this is done, risk identification focuses on what could still go wrong (WCGW), despite the existing controls. This process is intended to identify risks that are not already being addressed by existing controls. Managers and auditors then can determine whether to accept an individual risk or to establish new controls to mitigate it.

The residual risk format avoids the shortcomings of the inherent risk matrix. Identifying controls first decreases the temptation to identify ineffective controls as WCGWs. Instead, auditors will find ineffective controls when they test the operational effectiveness of the key existing controls. Managers also prefer the residual risk matrix because it treats them like good managers with good controls in place and focuses on what else could go wrong.

Some auditors have rejected the residual risk matrix method because it is not the approach demonstrated by COSO in its internal control framework. For example, the Evaluation Tools volume presents a risk matrix (Risk Assessment and Control Activities Worksheet) that lists inherent risks before controls. However, COSO is careful to state that such tools are only examples to demonstrate the concepts; they are not requirements or best practices, nor are they part of the framework. Another thing to remember about the COSO format is that risks and objectives are only related to the Risk Assessment and Control Activities components of that framework — the Control Environment, Information and Communication, and Monitoring components are different types of control that must be present to have an effective system of internal controls.

Other auditors believe a risk-based audit approach requires them to identify risks first. But risk-based auditing refers to how auditors select audits (annual audit planning) and the need to focus on the most important areas within an audit. In that sense, risk-based auditing may be easier to understand as "importance-based" auditing. The residual risk matrix approach is still risk-based, and there's no requirement that auditors must identify risks first. By identifying what could still go wrong, auditors identify uncontrolled (residual) risks and responses to those events.

Finally, many auditors argue that if they don't begin by identifying risks in the matrix, they won't know if the right controls are in place. However, identifying controls and what could still go wrong will reveal any wrong or missing controls related to objectives and risks. In fact, many auditors who use the inherent risk

matrix complete the controls or response to risks column first, and then fill in the risk column — effectively using the residual risk method.

Room For Both Formats

Experienced auditors know there is more than one way to perform an audit task, and some tools are more suited to some situations than others. Risk matrices are no different. The "Objective–Risks–Responses" format of a risk matrix, or an inherent risk analysis, is best used with high-level business objectives, such as increasing market share or maximizing revenues, where there are few specific controls or responses already in place. On the other hand, using the inherent risk matrix where many controls are already in place, leads to the shortcomings above. Because most audits are performed in established areas where systems and processes exist, the residual risk approach of identifying controls first, then asking what could still go wrong, can save audit time and lead to a more positive product.

An example Residual Risk Matrix is available in the features section of Internal Auditor*'s Web site, www.internalauditoronline.org. See Below.*

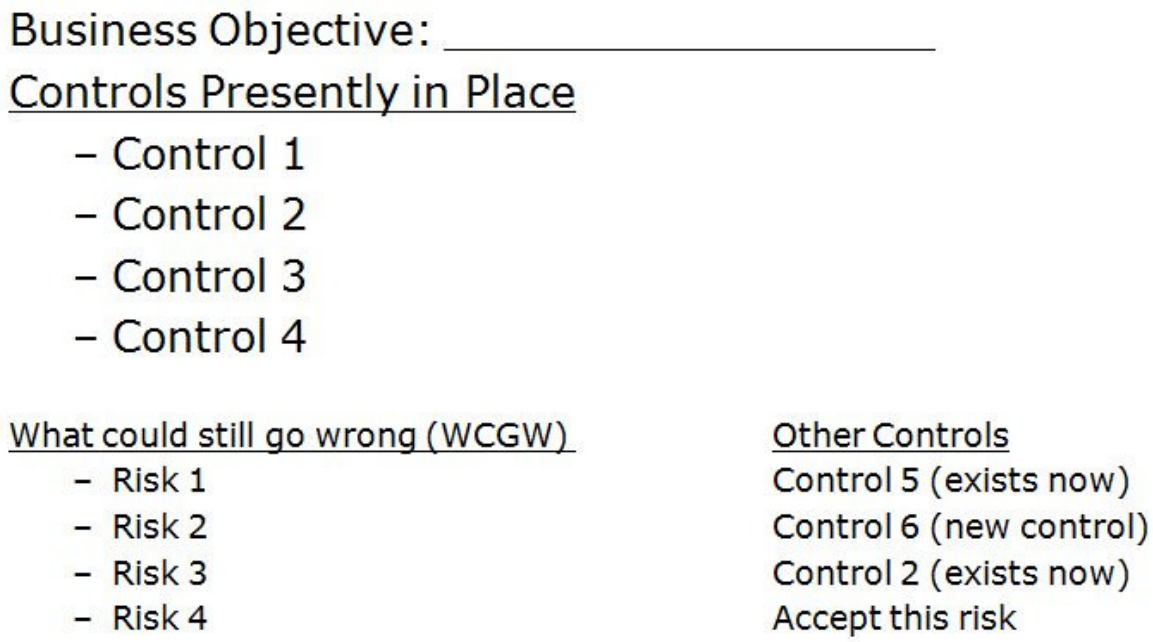
Larry Hubbard, CIA, CPA, CISA, CCSA, is principal of Larry Hubbard & Associates, an auditor training company based in Bethesda, Maryland.

[Online Sidebar: The Residual Risk Matrix

A risk matrix is a commonly-used tool for documenting the analysis of objectives, risks, and responses. Typically a risk matrix focuses first on the inherent risks related to an objective — that is, all the risk events that could have an impact on achieving the objective, without regard to management's responses. The typical inherent risk matrix lists these risk events, along with a risk rating (e.g., high, medium, or low) of their potential impact and likelihood. Next, the matrix identifies management's response (i.e., controls) to each event and determines the overall adequacy of the design of controls. The central question of this assessment is, considering the risks identified and the responses management has in place to mitigate, or control, the risk events, is there a reasonable likelihood that the objectives will be achieved? Based on this assessment, auditors prepare an audit program to test the operational effectiveness of controls.

However, using a residual risk analysis approach that starts by identifying controls can make the risk matrix process more effective and efficient. In almost all processes and activities, identifying what already exists first is a more direct method. Plus, it is a more positive experience for auditors and managers, because the approach looks for good things first (controls) rather than bad things (risks).

The residual risk approach starts with identifying the controls in place to achieve an objective. In this diagram, Controls 1 through 4 already exist and are identified during the audit interviewing process or self-assessment workshops. In asking "What could still go wrong" (WCGW), auditors and managers are trying to identify risks that are not already being addressed by existing controls. In this diagram, Control 5 already exists in another area and helps to mitigate Risk 1 — the auditors just did not identify it earlier. Control 6 is a new control that auditors and managers have determined needs to be implemented to mitigate Risk 2 (this may be among the "findings" of the audit). Control 2, which the auditors had already identified, mitigates Risk 3. Finally, management has decided to accept Risk 4 since this residual risk is within management's tolerance level for that risk.



A typical inherent risk matrix format is below.

Risk Matrix

Business Objective _____

Risks	Risk Rating (H,M,L)	Response to Risk	Adequacy

In this format, all important risk events that could impact achieving a business objective are listed, along with a Risk Rating (High, Medium, or Low) of the potential impact and likelihood of each event. Then, management's response to each event is identified, and the overall adequacy of the design of controls is determined. That is, how likely is the objective to be achieved, considering the risks identified and the responses management has in place to mitigate, or control, the risk events? After this evaluation of "design adequacy," auditors would prepare an audit program to test the "operational effectiveness" of controls.

End of article