Risk assessment: go big or go small?

Highlights

- Risk assessments fall into two categories: enterprise-level and business process-level.
- When looking only at big-picture risks, you might miss some program risks.
- If your organization spends all its time focused on risk at the business process-level, it may miss critical global risks.
- To mitigate all the risks your organization faces, you will have to think about both enterprise-level risks and business process-level risks.

Risk assessments fall into two categories: enterprise-level risk assessments and business process-level risk assessments. Enterprise-level risk assessments take an organization’s strategic risks into account. For example, they might look at the changing demographics of stakeholders or the status of aging facilities. Business process-level risk assessments focus on the risks in a specific area, such as payroll or accounts receivable.

These two approaches might lead you to wonder which is best. Should you do an enterprise-level risk assessment or a business process-level risk assessment? The answer is “Yes!” You should do both.

Here is why: Imagine you recently bought a home. You had some concerns about the house when you were considering the purchase, so you hired a home inspector. The inspector assessed whether the home was well insulated. She checked if the roof leaked. She looked into whether the foundation was sound. Satisfied that everything checked out, you happily purchased the home.

Now it is a month later and you have settled into your new home. You arrive home from work one evening to find that the toilet has clogged, overflowed, and flooded your basement. Worse yet, your kid left the front door open when they went to school in the morning, allowing all the heat in the house to escape and pipes to freeze.

While your home was basically sound, problems in specific areas caused massive disruption. Your roof did not leak, yet your home still flooded. Your home was well insulated, yet heat escaped.

As with our home analogy, your organization may have looked at big-picture risks but might still be missing risks in certain areas. For example, perhaps you identified an older grants management system as an enterprise-wide risk. You might try to mitigate this risk by buying a new system. But what if after you launch the system, a grants worker has unlimited administrative rights? What if this person decides to start self-approving funds to fraudulent grants recipients?

The converse of this situation is also true. If your organization spends all its time focused on risk at the business process-level, it may miss critical global risks. In this case, you could have the entire grants management system user roles mapped and controlled, but the software is so old that the software company no longer provides security patches. This leaves it vulnerable to cyberattack and crashes.

To really mitigate all the risks your organization faces, you need to think about both enterprise-level risks and business process-level risks. A strong system of internal control includes both a macro and a micro understanding of risk.

Suggested action steps: Have most of your risk assessments been enterprise-wide or have they been business process-specific? Consider diversifying the scope of your next risk assessment effort. Talk to the Internal Control and Accountability team if you would like help scoping your next risk assessment.

If you have questions, please contact Mike Thone at 651-201-8132.

COSO Pyramid used with permission. Copyright 1992-2009. Committee of Sponsoring Organizations of the Treadway Commission. All rights reserved.

Distributed by Minnesota Management and Budget
658 Cedar Street | Centennial Office Building
St. Paul, Minnesota 55155