

## Are you aware of your third-party risks?

### Highlights

- When well-managed, third-parties help your agency achieve its objectives.
- Using a third-party reduces management's direct control and increases the need for oversight.
- Consider third-party risk as part of your agency's control environment self-assessment.

Now that it is summer, is your grass getting a little long, overgrown, and out of control? No time to mow it? Save some time and potential frustration by outsourcing the lawn mowing to a third-party, like a lawn service or that neighbor kid down the street trying to make some extra money! Just be sure you have considered and weighed all the risks, because you will be at the mercy of whomever you hire! Whether you go with a lawn service or the neighbor kid, some risks can include: a damaged lawn (fertilizer dead spots or burnt patches), un-mowed spots or entire sections, grass clippings everywhere (sidewalk, driveway, street, etc.), and an untimely death for your begonias. You may find that the third-party does not do as good of a job as you would, but outsourcing is still saving you some time. Question is, if it is really worth the risk of losing your flower garden over it?

Both private and public sector organizations are increasingly relying on outsourcing to third-parties to carry out vital business functions. In fact, the U.S. Government alone spends an estimated \$550 billion annually on outsourced products and services. A third-party is anyone outside your agency including, vendors, contractors, and grantees, that provide a product or service to, or on behalf of, your agency. When managed appropriately, outsourcing can be an efficient and cost effective way to meet agency objectives. However, using a third-party also creates new risks and potential non-compliance issues that can lead to fines, lawsuits, and reputational damage. Some common questions to ask when evaluating third-party risks include:

*Strategic* – Does the third-party share your agency's strategic vision?

*Reputation* – Does the service provider have a good reputation? Will they do a good job or damage the agency's reputation with poor quality work or service?

*Operational* – Does the third-party have an up-to-date business continuity and disaster recovery plan? Has it been tested recently?

*Transaction* – Has the service provider ever been unable to deliver its product or provide its service due to error, fraud, or technology failure?

*Credit* – Has the third-party been unable to meet the terms of any past or current contractual obligations?

*Compliance* – Does the service provider have any history of non-compliance with the law, rules, or regulations? Are they in compliance with the agency's own internal policies, procedures or business standards?

Assessing and managing third-party risk takes a team effort. Management and agency employees must continually monitor the agency's outsourced relationships throughout the life of the contract. The use of a third-party reduces management's direct control over the activities outsourced and increases the need for oversight. All agency business process areas including, finance, compliance, legal, procurement, and business operations should assess and monitor third-party risk as it relates to their daily business processes.

You should consider third-party risk as a part of the agency's annual control environment self-assessment. The key to an agency's effective use of outsourcing is to appropriately assess, measure, monitor, and control the risks associated with the relationship.

*Suggested action steps:* Have you identified all your third-party relationships? What risks do those relationships bring to your agency? How do you monitor third-party relationships and manage the risks associated with them?

If you have questions, please contact Heidi Henry at [Heidi.Henry@state.mn.us](mailto:Heidi.Henry@state.mn.us) or (651) 201-8148.