



Ready, set, identify risks!

- **Inherent risk is the risk an activity or asset poses if no controls or other mitigating factors are in place.**
- **Activities or assets with high inherent risk have a greater potential for loss due to fraud, waste, unauthorized use, misappropriation, errors or violations of law.**
- **Characteristics to consider when assessing inherent risk include opportunity, unfamiliarity and complexity.**

Many of us struggle with the concept of *inherent risk*, meaning the risk an activity or asset poses if no controls or other mitigating factors were in place. Rather than identify the risks inherent to an asset or activity based strictly on its particular characteristics, we cannot seem to stop ourselves from considering existing controls, conclude that the risk is no longer a concern, then exclude the risk from further deliberation. For example, you might conclude there is little risk of someone breaking into your home because you lock your doors and windows before leaving.

One disadvantage to limiting risk identification in this way is that we lose the ability to see a complete picture of the risk landscape. Inherent risk identification provides a way to measure all risks—big and small—on equal footing. From this baseline, we can focus on the risks most likely to disrupt or derail an agency from achieving its mission, goals and objectives. This vantage point allows us to take a fresh look at existing control activities to ensure that high inherent risks are being mitigated as intended. And in an era of increasingly limited resources, it allows us to allocate those limited resources on the risks that matter most.

Activities or assets with high inherent risk have a greater potential for loss from fraud, waste, unauthorized use, misappropriation, errors or violations of law. Some characteristics that contribute to increased inherent risk are:

Opportunity:

- The potential for fraud increases when an asset is liquid or mobile. Examples include laptop computers, cell phones, cash, blank check stock and purchasing cards.
- Access to sensitive information, such as nonpublic data, increases the risk of identity theft and unauthorized use. The act of accessing protected information – even if that information is not “used” for anything – can present a risk to the agency.

Unfamiliarity:

- The newer or less frequent an activity, the greater the possibility that its operation and vulnerabilities may not be well understood, increasing the risk of errors and misappropriations. Any non-routine activity, if done infrequently, can be misunderstood or be conducted “off the radar”, making it more susceptible to error or misappropriation.
- Losing one or more key employees can greatly reduce productivity, lessen the ability to maintain expected service levels such as timeliness and accuracy, and increase the potential for errors or fraud.

Complexity:

- The more complex an activity is, the greater the possibility of errors occurring. For example, lengthy and complex requirements governing a large federal program may increase the likelihood of significant noncompliance and eligibility concerns.
- Account balances based on complex estimates or modeling are more likely to be erroneous than account balances based on simple estimates or routine, factual transactions.

Change:

- Significant process changes, such as converting to a new software application, can introduce new risks and/or make existing controls inoperable or no longer effective.

Suggested action steps: Do your risk assessment procedures include identification of inherent risks? Are you expending resources to control assets/activities that would be better spent controlling assets/activities with higher inherent risk?

If you have questions, please contact Jo Kane at Jo.Kane@state.mn.us or (651) 201-8174.