



## Demystifying risk assessments

- **Although we think about and assess risk every day at work, the process is usually informal and not documented.**
- **A risk assessment consists of four basic elements.**
- **In order to fully comply with the COSO Framework, you must document your key work-related risk assessments.**

To many people, risk assessments (the second component of the COSO Internal Control Framework) are a mystery. That is not because they don't understand risk—everyone has to think about and assess risk every day—but because this information is rarely written down or structured. COSO helps employees handle workplace risk by providing a framework for documenting risk assessments.

In this bulletin, we break down the risk assessment process into its four basic elements:

1. Figuring out what needs to be done,
2. Identifying things that can go wrong,
3. Prioritizing what can go wrong, and
4. Formulating actions that will reduce the chance that things will go wrong.

The risk assessment process begins by figuring out what needs to be done and how it needs to be accomplished. The what is the broad objective or goal which can be anything from getting to work to delivering services to thousands of Minnesotans. The how is the practical steps required to achieve that broad goal. In government, a legislative body typically sets broad program objectives such as building a road network, while state employees determine how to do so. In effect, the legislative and executive branches create a “to-do” list for achieving state goals.

Every item on your agency's to-do list has risks associated with it. A risk is anything that can go wrong or stand in the way of achieving a desired goal. Because there is an endless list of things that can go wrong, it is helpful to focus on the following categories: the failure to:

follow laws and regulations (compliance), account for activities (financial reporting), have sufficient personnel, equipment, or funding (operations), or protect physical or intangible state assets (safeguarding assets).

An attempt to address all identified risks equally could lead to paralysis and a waste of resources. To avoid this, the risks must be prioritized, or ranked. Prioritization is effective if criteria have been established for what differentiates a high risk (e.g. loss of a grant) from a low one (e.g. a slight project delay). The ranking scheme used should suit the circumstances of the organization.

There are three ways to react to risk: elimination, mitigation, and/or acceptance. It is difficult to completely eliminate a risk. Instead, risks are often mitigated to a point where the remaining risk is acceptable to the risk taker. Examples of risk mitigation include personal actions like wearing a seat belt (risk of injury in case of an accident) or office procedures such as supervisory approval of timesheets (risk of making inaccurate payroll payments).

*Suggested Action Steps:* Think about the goals of a program you work with. List some potential risks to achieving those goals. What activities are in place to mitigate the most important potential risks?

If you have questions, please contact John Nyanjom, Internal Control Specialist at (651) 201-8174 or [John.Nyanjom@state.mn.us](mailto:John.Nyanjom@state.mn.us).