

[REDACTED]

From: D Webster [REDACTED]
Sent: Wednesday, July 3, 2024 9:48 AM
To: Green Book Comments
Subject: Comments on Green Book revision

[REDACTED] [REDACTED]

CAUTION EXTERNAL EMAIL: Do not click on any links or open any attachments unless you trust the sender and/or know the content is safe. If you are suspicious of the e-mail, click on the Report Suspicious Emails button.

Mr. Dalkin:

The Greenbook has always had the following statement, which is unchanged in this proposed update:

“OV1.01 Internal control is a process effected by an entity’s oversight body, management, and other personnel, designed to provide reasonable assurance that the objectives of an entity will be achieved (see fig. 2).”

Unfortunately, this statement is overly broad and potentially confusing to those seeking to understand risk management beyond internal controls. In many cases, effective internal controls alone are insufficient to ensure achievement of organizational objectives.

Risk, per ISO 31000, is defined as the “the effect of uncertainty on objectives”. This uncertainty can stem from sources either internal to the organization (e.g., internal business processes or management decisions), or external to the organization (e.g., changing customer needs, changing sources/amounts of resources budgeted for an agency by Congress, changing political support, etc.). Moreover, a changing environment within which an organization operates effectively today may change and result in future challenges and risks not currently present. An organization can have effective internal controls over internal business processes today, but those objectives still may not be achieved because of risks occurring in the changed future environment or stemming from outside the organization. Organizations would want to foresee potential future risks and take appropriate actions, even if a change in current internal controls was not warranted.

The definition of internal control should thus be updated to clarify that it is designed to provide reasonable assurance that the organization’s existing processes are designed to support the achievement of objectives. However, that assurance of well operating business processes is not in and of itself sufficient to ensure all organizational objectives are met. Internal controls are but a part of a larger conversation in the management of risk, even if a very important part of that conversation.

Regards,

Douglas Webster, DBA

[REDACTED]