Risk advisory services
MBAF
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

17 May 2017
2017-08

Fill the GAAP
Providing you relevant updates on the latest financial reporting developments

The New AICPA Standard: Evaluating Cybersecurity Risk Management Programs

In response to growing market demand from customers, vendors, business partners and regulators for useful information about an entity's cybersecurity risk management efforts, the AICPA has expanded the options available for organizations to voluntarily report to external parties about the effectiveness of their cybersecurity risk management programs.

Entities now have the ability to provide cybersecurity assurance tailored to the informational needs of interested parties through newly developed criteria specifically defined to assess an organization's cybersecurity risk management program as well as through the recently updated Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.

In its officially released publication entitled *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (April 15, 2017), the AICPA unveils a reporting framework for a cybersecurity risk management examination. This examination is to be performed in accordance with the AICPA attestation standards and the AICPA cybersecurity guide. The AICPA defines nine categories of description criteria, also known as benchmarks, used to evaluate the process by which an organization manages its cybersecurity risks and the effectiveness of related cybersecurity controls. Through the use of common criteria, the comparability of the communication is enhanced. The description criteria are based on:

- The nature of the business and operations;
- The nature of information at risk;
- The objectives of the cybersecurity risk management program;
- Other factors that may have a significant effect on inherent cybersecurity risks;
- The organization's cybersecurity risk governance structure;
- The organization's cybersecurity risk assessment process;
- The cybersecurity communications and the quality of cybersecurity information;
- The monitoring of the cybersecurity risk management program; and
- The cybersecurity control processes.

Cybersecurity examination results based on these criteria are intended for internal and external stakeholders whose decisions might be affected by the effectiveness of the organization's cybersecurity program.

Updated Trust Services Criteria

Since the reporting framework is flexible, organizations still have the option to evaluate the suitability of design and operating effectiveness of controls included in their cybersecurity risk management program using the updated Trust Service Principles defined by the AICPA (security, availability, processing integrity, confidentiality and privacy) The revised criteria are now more closely aligned with the 17 principles in the 2013 internal control framework issued by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission. This will allow accounting professionals to better assist clients by incorporating the cybersecurity risk management program into the company's overall internal control framework.

Important Considerations

- Organizations interested in pursuing a third party attestation through a cybersecurity risk management examination are strongly encouraged to use the newly defined description criteria as a guide to develop their cybersecurity risk management program description. Given the relatively short experience with such evaluations, organizations are encouraged to perform diagnostic assessments to identify potential reportable exceptions that may lead to qualified opinions.
- The revised attestation standards are intended to be scalable and non-prescriptive, which allow organizations the flexibility to use sets of criteria other than those presented within the AICPA's Trust Services Principles as long as these are "suitable". Other viable sets of criteria include the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) or ISO's Information Security Management framework (ISO 27001). Official mappings of the AICPA's Trust Services Criteria to these widely used frameworks are available from the AICPA website.
- Whereas SOC 2 reports continue to be restricted use reports intended for specified parties, reports resulting from the new cybersecurity risk management examination are appropriate for general distribution.
- Given the subject matter of the attestation, independent public accountants are strongly encouraged to work with information security specialists and experienced IT audit practitioners in the evaluation of cybersecurity risk management programs and underlying controls.
- The independent opinion resulting from a cybersecurity risk management examination is not a guarantee against potential cyber attacks. Instead, the opinion is meant to communicate that the assessed entity has controls in place to detect and respond to cybersecurity threats under reasonable circumstances.

We can help

With the rapid evolution of threats in the cybersecurity landscape, there has never been a greater need for organizations to evaluate the effectiveness of their cybersecurity programs and to communicate the results of these evaluations to interested stakeholders. The criteria presented above will allow management and their trusted accounting advisors to better prepare a company for a robust cybersecurity risk management program. Our team of experienced IT security professionals are ready to answer your questions about how to leverage these new criteria within your organization. Feel free to contact our team below.

Risk advisory services

MBAF

CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

17 May 2017
2017-08

About us

MBAF's Risk Advisory Services practice strives to help manage risks and improve operations within your business. We work with all organizations to help realize business opportunities in complex issues, respond to key market and financial reporting developments and deliver distinctive results.

We serve domestic and international clients across a broad range of industries and practices in more than 44 countries and all 50 states from our offices in New York, Valhalla, Miami, Fort Lauderdale, Boca Raton, Orlando, Baltimore, Boulder, Las Vegas, our overseas office in Ahmedabad, India, and through our independent affiliate network at Baker Tilly International.

Contact us

Jesus Socorro
Managing Principal - Risk Advisory
212.931.9167
jsocorro@mbafcpa.com

Alvaro Florez
Principal – Risk Advisory IT
786.507.5884
aflorez@mbafcpa.com

Jorge Santiago
Senior Manager – Risk Advisory IT
786.347.3883
jsantiago@mbafcpa.com