SOC for Cybersecurity

Evaluating an entity-level cybersecurity risk management program

June 2017

As the information security landscape continues to evolve and cyber risks and threats become more sophisticated, the demand for mechanisms to evaluate and report on the controls organizations have in place to manage cybersecurity risks has steadily increased.

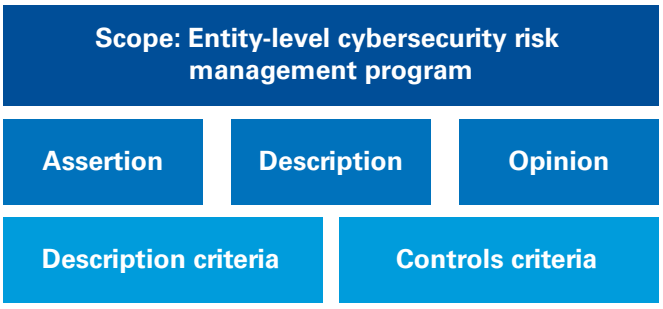
Overview

The information security landscape continues to evolve and cybersecurity risks are at the forefront of organizations' business issues as they consider their risk posture and potential exposure. Organizations' effective and secure interaction with business partners, vendors, and service organizations are critical to the efficient operation of business processes. Companies have implemented cyber risk management programs to address these risks but often struggle to obtain and share cybersecurity risk management information internally and externally.

In response to growing challenges related to cybersecurity risk management, the American Institute of CPAs (AICPA) has developed an entity-level cybersecurity risk management reporting framework (the Framework) that organizations can use to communicate relevant and useful information about the effectiveness of their cybersecurity risk management program to a broad range of stakeholders[1]. The initiative springs from the public accounting profession's commitment to continuous improvement, public service, and increasing investor confidence.

This new Framework affords companies the ability to provide key information about the effectiveness of an organization's cybersecurity risk management program that can be useful to boards of directors, senior management, and other pertinent internal and external stakeholders.

Components of the framework



[1] *Cybersecurity: How CPAs and their Firms Are Addressing a Dynamic and Complex Risk*, Center for Audit Quality, April 2017

What is new

The Framework provides a common approach to evaluating and reporting on an entity's cybersecurity risk management program. The resulting cybersecurity examination report, System and Organization Controls (SOC) for Cybersecurity, is comprised of three sections. These include management's description of the cybersecurity risk management program (program); management's assertion regarding the description and effectiveness of the program's controls; and the independent auditor's opinion on the description and effectiveness of the program's controls to achieve cybersecurity objectives. The Framework also provides two sets of criteria for use by companies and the practitioner. The first is a set of description criteria that is used to assist management with the preparation of a consistent and comparable narrative description of their program. The second is the AICPA's revised Trust Services Criteria for Security, Availability, and Confidentiality (2017), which is a set of control criteria that can be used to evaluate the effectiveness of controls within the program. Finally, the AICPA has released a cybersecurity attestation guide to assist with the consistent performance and reporting for cybersecurity examinations.

The AICPA's description criteria provide the foundation for comparable and consistent reporting in the following areas:

- Nature of operations
- Nature of information at risk
- Cybersecurity risk management program objectives
- Factors that have a significant effect on inherent cybersecurity risks
- Cybersecurity risk governance structure
- Cybersecurity assessment process
- Cybersecurity communications
- Quality of cybersecurity information
- Monitoring of the cybersecurity risk management program
- Cybersecurity control processes

How it can be used

The Framework can used at all stages of preparing for and performing a cybersecurity risk management program examination by both company management and practitioners.

Cybersecurity risk management examination

An examination is performed using the description criteria, along with control criteria to evaluate the organization's cybersecurity risk management program. Companies prepare a description of their cybersecurity risk management program based on the AICPA's description criteria requirements. Additionally, companies select suitable control criteria which are used to evaluate the controls within the cybersecurity risk management program. Companies may choose to use the AICPA's revised Trust Services Criteria for Security, Availability, and Confidentiality (2017) or they may choose to use other established control criteria such as the NIST Critical Infrastructure Cybersecurity Framework, or ISO 27001/27002, as long as such criteria are appropriate in accordance with the AICPA's attestation standards. Management also provides an assertion regarding the presentation of the description of their cybersecurity risk management program and the effectiveness of its controls. The independent auditor, following the AICPA attestation standards, examines and reports on management's description of the cybersecurity risk management program and the effectiveness of the program's controls. Upon conclusion, the auditor's opinion is incorporated in the SOC for Cybersecurity report.

Readiness assessment

Many organizations today may not yet be prepared to undergo an entity-level examination due to the complexity, volume, and dynamic nature of their information systems. The SOC for Cybersecurity Framework can be a valuable tool in assisting companies prepare for an examination or for communicating to senior management the state of its cybersecurity risk management program. Experienced cybersecurity risk and control practitioners can use the Framework and criteria to perform a readiness assessment of an organization that can help management identify areas in their cybersecurity risk management program that may need remediation or simple documentation enhancements.

Remediation

Organizations may also seek assistance from cybersecurity practitioners with design and remediation of cybersecurity controls prior to an examination engagement performed by an independent auditor.

How KPMG can help

KPMG LLP (KPMG) has a long history of assisting organizations by evaluating controls and providing third-party assurance to help demonstrate the integrity of their control environment. Our teams are experienced in conducting independent SOC 1 examinations on controls relevant to user organizations' internal control over financial reporting; SOC 2 examinations over security, availability, processing integrity, confidentiality, and privacy, and other security and control-related attestation examinations.

KPMG uses multidisciplinary teams that are experienced in cybersecurity, risk and control frameworks, and examination-level attestations. KPMG can assist organizations from assessing controls to transforming their cybersecurity programs to support business-enabling platforms while maintaining the confidentiality, integrity, and availability of critical business functions and data. KPMG's professionals have substantial experience strategically aligning our client's business priorities with risk management and compliance needs.

KPMG is a leader in information security advisory services as recognized by an independent research firm. Our capabilities and multidisciplinary experience enable us to advise companies on their cybersecurity risk management programs. In order to effectively prepare for, or perform a SOC for Cybersecurity examination, we involve the right professionals with the relevant technical backgrounds, certifications, and competencies.

KPMG can help companies in evaluating their options for assessing and reporting on their cybersecurity risk management program to both internal and external stakeholders. We can also assist companies in preparing for a SOC for Cybersecurity examination by performing a readiness assessment or assisting with remediation activities. For additional information, please reach out to us using our contact information below.

Other resources

For additional information on the AICPA Cybersecurity initiative, refer to the AICPA's Web site at http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

Chris Mottram
Partner
T: 404-979-2100
E: cmottram@kpmg.com

Eddie Holt
Partner
T: 214-840-2116
E: eeholt@kpmg.com

David Palmer
Managing Director
T: 216-875-8171
E: davepalmer@kpmg.com

Glenn Siriano
Principal
T: 203-406-8242
E: gsiriano@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia